

IMPLEMENTASI KODE GOPPA PADA KRIPTOSISTEM MCELIECE

SKRIPSI

**OLEH:
LILI KHOIRIYAH
NIM. 200601110024**



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

IMPLEMENTASI KODE GOPPA 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:
LILI KHOIRIYAH
NIM. 200601110024**

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

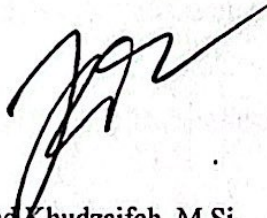
IMPLEMENTASI KODE GOPPA PADA KRIPTOSISTEM MCELIECE

SKRIPSI

Oleh:
Lili Khoiriyah
NIM. 200601110024

Telah Disetujui untuk Diuji
Malang, 3 Desember 2024

Dosen Pembimbing I



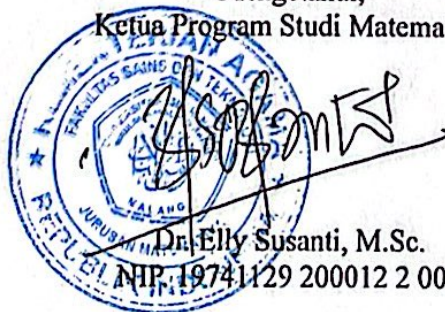
Muhammad Khudzaifah, M.Si.
NIPPPK. 19900511 202321 1 029

Dosen Pembimbing II



Erna Herawati, M.Pd.
NIPPPK. 19760723 202321 2 006

Mengetahui,
Ketua Program Studi Matematika



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

IMPLEMENTASI KODE GOPPA PADA KRIPTOSISTEM MCELEICE

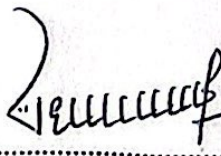
SKRIPSI

Oleh:
Lili Khoiriyah
NIM. 200601110024

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

Malang, 11 Desember 2024

Ketua Penguji : Evawati Alisah, M.Pd



.....

Anggota Penguji 1 : Mohammad Nafie Jauhari, M.Si



.....

Anggota Penguji 2 : Muhammad Khudzaifah, M.Si



.....

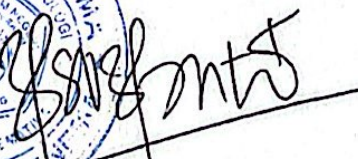
Anggota Penguji 3 : Erna Herawati, M.Pd



.....

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 : Lili Khoiriyah

NIM : 200601110024

Program Studi : Matematika

Fakultas : Sains dan Teknologi

Judul Skripsi : Implementasi Kode Goppa 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, 11 Desember 2024



Lili Khoiriyah

NIM. 200601110024

MOTO

“Sesungguhnya Bersama Kesulitan Ada Kemudahan”

(Q.S Al-Insyirah: 5)

Hidup bukan untuk saling mendahului, bermimpilah sendiri-sendiri.

(Baskara Putra)

PERSEMBAHAN

Skripsi ini penulis persembahkan kepada:

Cinta pertama dan panutanku, Ayahanda Mahmudin. Beliau memang tidak sempat merasakan pendidikan sampai bangku perkuliahan, namun beliau mampu mendidik, memotivasi, dan memberi dukungan hingga penulis mampu menyelesaikan studinya sampai sarjana.

Pintu surgaku, Ibunda Jamilah. Beliau sangat berperan penting dalam menyelesaikan program studi penulis, berkat semangat, motivasi serta do'a yang tidak pernah terhenti hingga penulis mampu menyelesaikan pendidikan sampai sarjana.

Kakak Ahmad Muzaki dan Ahlun Najjah dengan kasih sayangnya memberikan do'a dan dukungan kepada penulis.

Terakhir, teruntuk diri saya sendiri Lili Khoiriyah. Terimakasih karena sudah memutuskan untuk tidak menyerah dalam keadaan apapun dan sudah bertahan sejauh ini.

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT. Karena limpahan rahmat serta karunia-Nya, sehingga penulis masih diberikan anugerah kesehatan, kesabaran, dan semangat dalam pembuatan skripsi dengan judul “Implementasi Kode Goppa pada Kriptosistem McEliece” dengan baik. Sholawat serta salam senantiasa selalu tercurahkan kepada Nabi Muhammad SAW yang selalu dinantikan syafaatnya di yaumul akhir.

Dalam penyusunan skripsi, penulis mendapat bantuan, dukungan, bimbingan, dan motivasi dari berbagai pihak. Oleh karena itu ucapan terima kasih penulis sampaikan kepada yang terhormat:

1. Prof. Dr. H. M. Zainuddin, M.A., selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim Malang.
2. Prof. Dr. Sri Harini, M.Si, selaku dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
3. Dr. Elly Susanti, M.Sc, selaku ketua Program Studi Matematika, Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. Muhammad Khudzaiyah, M.Si., selaku dosen pembimbing I yang telah memberikan banyak arahan, nasihat, motivasi kepada penulis sehingga dapat menyelesaikan penyusunan skripsi dengan baik.
5. Erna Herawati, M.Pd., selaku dosen pembimbing II yang telah memberikan bimbingan serta arahan kepada penulis sehingga dapat menyelesaikan penyusunan skripsi dengan baik.
6. Segenap civitas akademika Program Studi Matematika, Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang, terutama untuk seluruh dosen Matematika terimakasih atas segala ilmu dan bimbingannya.
7. Kedua orang tua dan kakak penulis yang selalu mendoakan dan memberikan dukungan penuh kepada penulis baik berupa materi maupun nonmateri, sekaligus nasehat-nasehat yang membangun sehingga menjadi motivasi bagi penulis selama menempuh pendidikan di bangku perkuliahan.

8. Pemilik NIM. 200601110101, yang telah kebersamai penulis selama di bangku perkuliahan dan menjadi *support system* terbaik selama proses pengerjaan skripsi.
9. Sahabat dekat penulis Aldina, Nanda, Ira, Afi yang selalu menjadi teman berproses dan selalu menjadi garda terdepan saat penulis membutuhkan bantuan. Terimakasih sudah menjadi keluarga penulis di perantauan.
10. Teman-teman satu bimbingan Lengga, Aam, Anggi dan Soviana yang senantiasa berbagi ilmu dan membantu penulis dalam penyusunan skripsi.
11. Seluruh mahasiswa matematika angkatan 2020 yang telah memberikan semangat dan dukungan dalam berbagai hal.
12. Serta semua pihak yang selalu mendukung serta memberikan semangat dalam penyusunan skripsi.

Semoga Allah SWT melimpahkan pahala yang berlipat ganda. Penulis memohon maaf jika terdapat kesalahan dalam proses penulisan. Semoga skripsi ini dapat bermanfaat bagi penulis dan para pembaca.

Malang, 11 Desember 2024

Penulis

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGAJUAN	ii
HALAMAN PERSETUJUAN	iii
HALAMAN PENGESAHAN	iv
PERNYATAAN KEASLIAN TULISAN	v
MOTO	vi
PERSEMBAHAN.....	vii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	x
DAFTAR TABEL	xii
DAFTAR GAMBAR	xiii
DAFTAR LAMPIRAN	xiv
ABSTRAK	xv
ABSTRACT	xvi
مستخلص البحث.....	xvii
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	5
1.3 Tujuan Penelitian.....	5
1.4 Manfaat Penelitian.....	5
1.5 Batasan Masalah.....	6
1.6 Definisi Istilah	6
BAB II KAJIAN TEORI	8
2.1 Teori Pendukung.....	8
2.1.1 Keterbagian.....	8
2.1.2 Bilangan Prima	8
2.1.3 Faktor Persekutuan Terbesar.....	9
2.1.4 Relatif Prima.....	9
2.1.5 Aritmatika Modulo	10
2.1.6 Kongruensi.....	10
2.1.7 Teorema Euler.....	10
2.2 Lapangan Hingga	11
2.2.1 Polinomial.....	11
2.2.2 Operasi Aljabar pada Polinomial.....	12
2.2.3 Lapangan Hingga dengan Elemen Polinomial $GF(2^n)$	13
2.2.4 Aritmatika Modulo Polinomial.....	14
2.3 Kode Linier	15
2.4 Matriks Generator dan Matriks Parity Check	16
2.5 Kode Goppa.....	17
2.6 Algoritma Petterson.....	18
2.7 Kriptografi.....	19
2.8 Sistem Kriptografi Kunci Publik.....	20
2.9 Kriptosistem McEliece	20
2.9.1 Pembangkitan Kunci.....	21
2.9.2 Proses Enkripsi	21
2.9.3 Proses Dekripsi	22

2.10 Kajian Integrasi Topik dengan Al-Qur'an/Hadits	22
2.11 Kajian Topik dengan Teori Pendukung	28
BAB III METODE PENELITIAN	29
3.1 Jenis Penelitian	29
3.2 Pra Penelitian.....	29
3.3 Tahapan Penelitian	30
BAB IV HASIL DAN PEMBAHASAN	32
4.1 Pembentukan Kunci	32
4.1.1 Algoritma Pembentukan Kunci pada Kriptosistem McEliece	32
4.1.2 Simulasi Pembentukan Kunci pada Kriptosistem McEliece	33
4.2 Proses Enkripsi	36
4.2.1 Algoritma Enkripsi Menggunakan McEliece	36
4.2.2 Simulasi Proses Enkripsi Menggunakan Algoritma McEliece	37
4.3 Proses Dekripsi.....	41
4.3.1 Dekripsi Menggunakan Algoritma McEliece dengan Kode Goppa.	41
4.3.2 Simulasi Proses Dekripsi Menggunakan Algoritma McEliece	42
4.4 Analisis Hasil	69
4.5 Kajian Integrasi Agama	70
BAB V PENUTUP	72
5.1 Kesimpulan.....	72
5.2 Saran.....	73
DAFTAR PUSTAKA.....	74
LAMPIRAN.....	76
RIWAYAT HIDUP.....	86

DAFTAR TABEL

Tabel 2.1 Operasi Penjumlahan Pada $GF(2^n)$	15
Tabel 2.2 Operasi Perkalian Pada $GF(2^n)$	15
Tabel 4.1 Representasi Polinomial $GF(2^4)$	33

DAFTAR GAMBAR

Gambar 2.1 Skema Kriptografi Kunci Publik.....	20
--	----

DAFTAR LAMPIRAN

Lampiran 1 Pesan asli dengan daftar simbol dan kode biner berdasarkan tabel ASCII.....	76
Lampiran 2 Hasil program <i>sagemath</i> untuk implementasi algoritma kriptosistem McEliece menggunakan kode Goppa $n = 12$ dan $k = 4$	76

ABSTRAK

Khoiriyah, Lili. 2024. **Implementasi Kode Goppa 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: Kode Goppa, Kriptosistem McEliece, Kriptografi

Penelitian ini mengimplementasikan kode Goppa pada kriptosistem McEliece untuk menghadapi ancaman komputer kuantum. Dengan menggunakan polinomial $g(x) = x^2 + a^7x + 1$ pada lapangan hingga $GF(2^4)$, menghasilkan parameter kode dengan panjang $n = 12$, dimensi $k = 4$, dan tingkat kesalahan $t = 2$. Proses enkripsi dilakukan dengan kunci publik G' dan penambahan *error* acak, sedangkan dekripsi menggunakan kunci privat untuk mendeteksi dan memperbaiki *error* melalui perhitungan *syndrome*. Kode goppa meningkatkan keamanan kriptosistem melalui kemampuan koreksi hingga $t = 2$ *error* berdasarkan properti polinomial pembangkitnya dan struktur matriks paritas H yang bersifat pseudorandom. Hasil penelitian ini menunjukkan bahwa kode Goppa meningkatkan keamanan kriptosistem McEliece melalui kemampuan koreksi *error* yang tinggi, sehingga menjadikan kriptosistem McEliece dengan kode Goppa sebagai solusi yang efektif dalam menjaga keamanan informasi di era kriptografi modern.

ABSTRACT

Khoiriyah, Lili. 2024. **The Implementation Goppa Code on McEliece Cryptosystem.** Undergraduate Thesis. Mathematics Department, Faculty of Science and Technology, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Advisors: (I) Muhammad Khudzaifah, M.Si. (II) Erna Herawati, M.Pd.

Keywords: Kode Goppa, McEliece Cryptosystem, Cryptography.

This research implements Goppa codes in the McEliece cryptosystem to address the threats posed by quantum computers. By utilizing the polynomial $g(x) = x^2 + a^7x + 1$ over the finite field $GF(2^4)$, producing code parameters with length $n = 12$, dimension $k = 4$, and error rate $t = 2$. The encryption process is performed using the public key G' and the addition of random errors, while decryption employs the private key to detect and correct errors through syndrome computation. Goppa codes enhance the cryptosystem's security by enabling correction of up to $t = 2$ errors, leveraging the properties of the generator polynomial and the pseudorandom structure of the parity-check matrix H . The results of this study demonstrate that Goppa codes significantly improve the security of the McEliece cryptosystem through their high error-correction capability, making the McEliece cryptosystem with Goppa codes an effective solution for safeguarding information in the era of modern cryptography.

مستخلص البحث

خيرية، ليلي. ٢٠٢٤. تنفيذ نظام تشفير *McEliece* باستخدام رموز غوبا. البحث الجامعي. قسم الرياضيات، كلية العلوم والتكنولوجيا بجامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج. المشرف الأول: محمد حذيفة، الماجستير. المشرف الثاني: إيرنا هيراواتي، الماجستير.

الكلمات الرئيسية: كود غوبا، نظام تشفير *McEliece*، التشفير.

هدف هذا البحث العلمي إلى تطبيق كود غوبا ضمن نظام التشفير *McEliece* لمواجهة التهديدات التي قد تنشأ نتيجة تطور الحوسبة الكمومية. باختيار كثير الحدود $g(x) = x^2 + a^7x + 1$ في الحقل $GF(2^4)$ ، تم الحصول على معلمات الكود بطول $n = 12$ ، وبعد $k = 4$ ، ومعدل تصحيح أخطاء $t = 2$. تمت عملية التشفير باستخدام المفتاح العام G' وإضافة أخطاء عشوائية، بينما يعتمد فك التشفير على المفتاح الخاص لتحديد الأخطاء وتصحيحها عبر حساب المتلازمات. يميز كود غوبا بقدرته على تحسين أمان النظام بفضل خاصية كثير الحدود المولد وهيكل مصفوفة التكافؤ العشوائي الزائف H . أظهرت نتائج الدراسة أن استخدام كود غوبا يعزز أمان نظام *McEliece* بشكل ملحوظ من خلال قدرته العالية على تصحيح الأخطاء، مما يجعله حلاً فعالاً في الحفاظ على أمن المعلومات في ظل تحديات التشفير الحديثة.

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Dalam era digital seperti sekarang ini, keamanan transmisi pesan menjadi salah satu masalah yang penting. Banyaknya penyalahgunaan pada proses transmisi pesan melalui jaringan internet, memerlukan peningkatan keamanan terhadap kerahasiaan suatu informasi. Penggunaan sistem digital untuk proses transmisi pesan jarak jauh merupakan pilihan terbaik. Namun ketika transmisi data harus melewati ratusan atau ribuan kilometer, potensi kesalahan (*error*) menjadi lebih tinggi (Anggraeni, 2004). Kesalahan dapat disebabkan oleh gangguan saluran atau gangguan dari luar yang mengakibatkan pesan yang dikirim berbeda dengan pesan yang diterima.

Permasalahan seputar transmisi data tidak berhenti sampai di sini. Mengikuti perkembangan teori pengkodean, muncul masalah keamanan terkait transmisi pesan yang dikirim melalui komputer atau jaringan internet. Keberadaan internet sebagai sarana umum, memungkinkan untuk diakses secara bebas. Akses internet gratis meningkatkan resiko penyadapan pesan oleh pihak yang tidak berwenang. Oleh karena itu, menjaga keamanan data atau informasi menjadi hal utama bagi pengguna internet dalam melindungi privasi mereka. Untuk menjaga kerahasiaan pesan, maka dibutuhkan mekanisme pengamanan pesan yang baik. Akhirnya dikembangkanlah ilmu yang memfokuskan tentang teknik pengamanan transmisi pesan yang kemudian dikenal sebagai kriptografi.

Kriptografi adalah ilmu matematika yang mempelajari metode-metode dan algoritma yang bersangkutan dengan keamanan pesan (Ariyus , 2008). Kriptografi merupakan ilmu menulis pesan rahasia untuk menyembunyikan pesan dengan cara mengubahnya menjadi kode tertentu sehingga kode yang dikirim menjadi tidak bermakna (Ziaurrahman, Utami, & Wibowo, 2019). Hal ini dilakukan untuk memastikan bahwa pesan yang disampaikan hanya dapat dimengerti oleh orang yang berhak untuk mengetahuinya, tanpa melibatkan pihak lain. Menjaga kerahasiaan pesan merupakan amanat yang penting agar isi pesan tersebut dapat tersampaikan dengan baik. Pentingnya menjaga amanat telah tercantum dalam Al-Qur'an surat Al-Anfal ayat 27:

يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَخُونُوا اللَّهَ وَالرَّسُولَ وَتَخُونُوا أَمْنَتِكُمْ وَأَنْتُمْ تَعْلَمُونَ ﴿٢٧﴾

Artinya: *“Hai orang-orang yang beriman, janganlah kamu mengkhianati Allah dan Rasul (Muhammad) dan juga janganlah kamu mengkhianati amanat-amanat yang dipercayakan kepadamu, sedang kamu mengetahui.”* (Q.S Al-Anfal:27)

Berdasarkan ayat di atas, menjaga amanat berarti memastikan bahwa pesan yang akan disampaikan tetap terjaga kerahasiaannya. Dalam merahasiakan pesan dibutuhkan sebuah metode kriptografi yang kuat. Seiring dengan perkembangan zaman, definisi kriptografi berkembang menjadi suatu ilmu tentang teknis matematis yang diterapkan untuk mengatasi tantangan keamanan seperti privasi dan otentikasi.

Dalam bidang kriptografi terdapat teknik matematis untuk melakukan proses enkripsi dan dekripsi. Teknik ini untuk mengubah data asli menjadi suatu kode tertentu agar informasi tidak terbaca oleh pihak lain yang tidak berhak (Prayitno & Nurdin, 2017). Salah satu metode enkripsi dan dekripsi yang digunakan pada ilmu

kriptografi adalah algoritma kunci publik atau algoritma kunci asimetri. Di mana algoritma asimetri ini menggunakan kunci publik sebagai pengenkripsian dan kunci privat sebagai pendekripsian (Waliprana, 2011). Mempertimbangkan kunci publik yang bersifat umum sehingga tidak aman terhadap serangan kuantum, sehingga kerentanan sistem *public-key* terhadap serangan tersebut menjadi suatu hal yang menarik.

Kriptosistem McEliece merupakan salah satu kandidat terbaik untuk standarisasi kriptografi *post-quantum* karena proses enkripsi pada kriptosistem McEliece ini menggunakan sifat acak (*randomization*). Terdapat dua jenis kunci dalam kriptosistem McEliece yaitu kunci privat dan kunci publik. Kunci privat menyimpan dekripsi kode linier yang bergantung pada generatornya, sementara kunci publik berupa matriks yang sedikit acak dari kode yang sama sehingga sulit untuk membedakan dengan kode linier yang benar-benar acak (Siim, 2015). Skema enkripsi ini dimodifikasi menggunakan varian “*Dual*” dari kode *Generalized Reed Solomon*, untuk memperbaiki ukuran kunci yang memberikan percepatan dalam implementasi perangkat lunak dan perangkat keras. Keamanan dalam Kriptosistem McEliece terletak pada kemampuan memulihkan teks biasa dari teks tersandi, menggunakan kode *error-correcting* yang tersembunyi.

Ada berbagai jenis kode *error-correcting* yang dapat digunakan untuk memperbaiki kesalahan yang mungkin terjadi selama transmisi data. Hal ini dilakukan dengan menambahkan redundansi yaitu informasi tambahan yang membuat pesan lebih mudah dipahami jika terjadi kesalahan. Namun, kesalahan tidak selalu terjadi secara kebetulan. Kesalahan juga dapat dengan sengaja di tambahkan untuk menyandikannya lebih lanjut. Dengan menggunakan algoritma

error-correcting dengan menambahkan vektor kesalahan akan mengacak pesan. Oleh karena itu dapat membuat sistem kriptografi menjadi lebih aman.

Kode Goppa merupakan salah satu jenis kode *error-correcting* yang relevan dalam sistem kriptografi. Kode ini didasarkan pada konsep dari sifat-sifat aljabar geometri untuk membangun kode tersebut. Kode Goppa memiliki jarak minimum aktual yang lebih besar dari dua kali jumlah kesalahannya. Sehingga dijamin memiliki kapasitas *error-correcting* yang tinggi sampai pada *error* tertentu. Selain itu, bentuk matriks *parity-check* pada kode ini juga sulit dibedakan dari matriks biner random. Hal ini menjadikan kode Goppa baik digunakan sebagai salah satu pilihan untuk meningkatkan keamanan pada kriptosistem *post quantum*.

Pada penelitian Wahyuni (2010) yang berjudul “Aplikasi Kriptosistem dengan Algoritma McEliece” menjelaskan bahwa algoritma McEliece dapat digunakan untuk penyandian yang efektif dengan kunci yang berbentuk matriks dan pada proses komputasinya. Penelitian ini juga menyebutkan untuk melipatgandakan keamanan algoritma ini dapat dikombinasikan dengan algoritma pertukaran kunci. Kemudian pada penelitian (Chen & Zhang, 2023) yang berjudul “*The number of extended irreducible binary Goppa codes*” menyebutkan suatu alasan kode Goppa memungkinkan untuk menahan serangan struktural apapun. Hal ini karena kode goppa memiliki sedikit invarian dan jumlah kode yang tidak setara bertambah secara eksponensial berdasarkan panjang dan dimensi kode. Sehingga pengetahuan tentang jumlah kode Goppa yang tidak setara untuk parameter tetap dapat memfasilitasi evaluasi keamanan sistem kriptografi tersebut.

Berdasarkan uraian di atas, maka penulis tertarik untuk melakukan penelitian yang berjudul “Implementasi Kode Goppa pada Kriptosistem McEliece”. Penelitian

ini dilakukan untuk menganalisis keamanan dan kerentanan dari kriptosistem McEliece saat diterapkan dengan kode goppa.

1.2 Rumusan Masalah

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

1. Bagaimana proses pembangkitan kunci McEliece dengan menggunakan kode Goppa?
2. Bagaimana proses enkripsi pesan dalam kriptosistem McEliece dengan menggunakan kode Goppa?
3. Bagaimana proses dekripsi pesan dalam kriptosistem McEliece dengan menggunakan kode Goppa?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dijelaskan sebelumnya, maka tujuan penelitian ini sebagai berikut:

1. Mengetahui proses pembangkitan kunci McEliece dengan menggunakan kode goppa.
2. Mengetahui proses dekripsi pada pesan menggunakan kriptosistem McEliece.
3. Mengetahui proses enkripsi pada pesan menggunakan kriptosistem McEliece.

1.4 Manfaat Penelitian

Adapun beberapa manfaat yang ada dipenelitian ini, adalah sebagai berikut:

1. Manfaat Teoritis

Penelitian ini diharapkan dapat untuk mengembangkan modifikasi pembangkitan kunci menggunakan kode goppa pada kriptosistem McEliece. Selain itu penelitian ini juga untuk memperbanyak bahan literasi dan informasi dalam lingkup ilmu kriptografi.

2. Manfaat Praktis

a. Bagi Penulis

- i. Memperoleh ilmu dan wawasan yang lebih dalam pada bidang kriptografi.
- ii. Menerapkan ilmu yang telah diperoleh dibangku perkuliahan, terutama pada bidang kriptografi.

b. Bagi Pembaca

- i. Mengetahui kandidat standarisasi kriptografi *post quantum* yang baik.
- ii. Memperoleh informasi yang dapat dikembangkan untuk penelitian dalam bidang kriptografi berikutnya.

1.5 Batasan Masalah

Batasan masalah yang akan dijelaskan dalam penelitian ini adalah konversi bilangan biner menggunakan tabel ASCII 256 karakter.

1.6 Definisi Istilah

Berikut istilah-istilah yang digunakan dalam penelitian ini:

Kode Goppa : Kode linier yang mengoreksi kesalahan yang dapat digunakan untuk mengenkripsi dan mendekripsikan pesan.

- Enkripsi : Proses mengubah suatu data atau informasi menjadi bentuk yang tidak dapat dipahami.
- Dekripsi : Proses pengubahan suatu data atau informasi yang tidak dapat dipahami ke bentuk semula.
- Kunci : Suatu parameter yang digunakan untuk mengendalikan jalannya algoritma kriptografi.
- Error Correcting* : Untuk menganalisis dan memperbaiki kesalahan pada proses pengolahan data.
- ASCII : Kode yang digunakan untuk mewakili karakter angka maupun huruf dalam komputer.

BAB II

KAJIAN TEORI

2.1 Teori Pendukung

2.1.1 Keterbagian

Definisi Misalkan $a, b \in \mathbb{Z}$, dengan $a \neq 0$, maka Bilangan bulat b dibagi habis oleh anggota bilangan bulat a (dinotasikan $a|b$) jika terdapat bilangan bulat c sedemikian sehingga $a = bc$ (Irawan, Hijriyah, & Habibi, 2014).

Contoh

$2|6$, karena terdapat $3 \in \mathbb{Z}$ sehingga $6 = 2 \cdot 3$

$3 \nmid 7$, karena tidak ada $c \in \mathbb{Z}$ sehingga $7 = 3c$

2.1.2 Bilangan Prima

Bilangan prima didefinisikan sebagai bilangan yang lebih besar dari 1 dan hanya dapat dibagi oleh 1 dan bilangan itu sendiri (Irawan, Hijriyah, & Habibi, 2014). Dapat disebutkan bahwa bilangan prima adalah suatu bilangan yang tidak dapat difaktorkan.

Definisi Misalkan $n \in \mathbb{Z}^+, n > 1$

1. n disebut bilangan prima jika n tidak memiliki pembagi positif selain 1 dan dirinya sendiri.
2. n disebut bilangan komposit jika n bukan bilangan prima.

2.1.3 Faktor Persekutuan Terbesar

Definisi Jika $a, b \in \mathbb{Z}$, maka bilangan p disebut faktor persekutuan terbesar dari a dan b jika p habis membagi a dan habis membagi b ($p|a$ dan $p|b$) (Sukirman, 2016).

Definisi Jika $a, b \in \mathbb{Z}$, yang keduanya tidak bersama-sama bernilai 0, maka faktor persekutuan terbesar dari a dan b adalah bilangan bulat positif p terbesar yang memenuhi $p|a$ dan $p|b$ (Sukirman, 2016).

Contoh

Faktor-faktor bilangan bulat positif dari 12 adalah 1, 2, 3, 4, 6, 12.

Faktor-faktor bilangan bulat positif dari 30 adalah 1, 2, 3, 5, 6, 10, 15, 30

Maka pembagi positif dari 12 dan 30 adalah 1, 2, 3 dan 6. Sehingga diperoleh $\text{FPB}(12, 30) = 6$.

2.1.4 Relatif Prima

Definisi Misalkan $a, b \in \mathbb{Z}$ dikatakan *coprime* atau relatif prima jika $\text{FPB}(a, b) = 1$ (Burton, 2011).

Contoh

20 dan 3 relatif prima karena $\text{FPB}(20, 3) = 1$.

Teorema Misalkan $a, b \in \mathbb{Z}$ dan $a, b \neq 0$. Maka a dan b adalah relatif prima jika dan hanya jika terdapat bilangan bulat m dan n (Burton, 2011).

$$ma + nb = 1$$

Contoh

Bilangan 20 dan 3 dikatakan relatif prima karena $\text{FPB}(20, 3) = 1$, atau dapat ditulis

$$2 \cdot 20 + (-13) \cdot 3 = 1$$

Dengan $m = 2$ dan $n = -13$.

2.1.5 Aritmatika Modulo

Teorema Misalkan $a \in \mathbb{Z}$ dan $m \in \mathbb{Z}$, $m > 0$. Maka dapat didefinisikan $a \bmod m$ sebagai sisa ketika a dibagi dengan m . Bilangan bulat m disebut modulus. Sedemikian sehingga $a = qm + r$ dengan $0 \leq r < m$ (Stallings, 2003).

Contoh

Berikut beberapa contoh operasi dengan operator modulo

$$1. 23 \bmod 5 = 3 \quad (23 = 5 \cdot 4 + 3)$$

$$2. 27 \bmod 3 = 0 \quad (27 = 3 \cdot 9 + 0)$$

2.1.6 Kongruensi

Definisi Jika $a, b, n \in \mathbb{Z}$, maka bilangan a dikatakan kongruen dengan b modulo n , jika dan hanya jika n membagi $(a - b)$ (Lapele, 2023).

ditulis $a \equiv b \pmod{n}$ jika dan hanya jika $n|(a - b)$.

Contoh

$n = 9$, $a = 33$, dan $b = 6$

$$a \equiv b \pmod{n}$$

$33 \equiv 6 \pmod{9}$, 9 habis membagi $33 - 6 = 27$.

2.1.7 Teorema Euler

Definisi Untuk setiap bilangan bulat yang relatif prima ke m , maka berlaku teorema euler berikut

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Dimana $\phi(m)$ adalah jumlah satuan modulo m , yang sama dengan jumlah bilangan a dengan $1 \leq a \leq m$ yang relatif prima terhadap m (Childs, 2019).

Contoh

Misalkan $a = 5$ dan $m = 16$ yang mana keduanya relatif prima, dan $\phi(m) = 8$, maka

$$5^8 \equiv 25^4 \equiv 9^4 \equiv 81^2 \equiv 1^2 \equiv 1 \pmod{16}$$

2.2 Lapangan Hingga

Lapangan Hingga adalah lapangan yang memuat jumlah elemen terbatas. Lapangan ini memungkinkan kita untuk menetapkan sesuatu tertentu pada sekumpulan angka, sehingga *field* diperlukan untuk memanipulasi angka.

Definisi Lapangan dengan jumlah elemen berhingga disebut *Finite Field* atau *Galois Field* ditulis $GF(q)$ dengan q sebagai ordo suatu *Field* (Artin, 1991).

2.2.1 Polinomial

Dalam bidang matematika, polinomial sering disebut sebagai suku banyak yang melibatkan jumlah perkalian pangkat dalam satu atau lebih variabel dengan koefisien. Polinomial $P(x)$ berderajat n , yang menunjukkan fungsi polinomial suku banyak dalam variabel x didefinisikan oleh fungsi berikut:

$$P(x) = \alpha_0 + \alpha_1x + \alpha_2x^2 + \dots + \alpha_nx^n, \quad \alpha_0 \neq 0$$

Bilangan bulat non negatif n disebut derajat polinomial, dan α_0 disebut koefisien utama. Jika $\alpha_0 = 1$, polinomialnya disebut *monic* yaitu polinomial yang memiliki koefisien pada pangkat tertinggi yang bernilai 1. Karena tidak terdapat

derajat pada polinomial nol, maka dapat dinyatakan bahwa derajat hasil kali dua polinomial adalah jumlah derajat polinomial tersebut (Niven, Zuckerman, & Montgomery, 1980).

2.2.2 Operasi Aljabar pada Polinomial

1. Penjumlahan

Pada operasi polinomial penjumlahan, perlu diperhatikan pangkat polinomialnya. Ada dua metode untuk menjumlahkan polinomial $f(x)$ dengan $h(x)$. Jika kita ingin menjumlahkan suku yang sejenis, maka kita dapat menggabungkan koefisien dari suku-suku tersebut, misalkan

$$f(x) = 6x^2 + 2x^2 = 8x^2$$

Sedangkan jika menjumlahkan suku yang berbeda, kita cukup menuliskan keduanya secara langsung tanpa perubahan. misalkan $6x^3$ dan $2x^2$ maka diperoleh $6x^3 + 2x^2$.

2. Pengurangan

Operasi polinomial pengurangan sama halnya seperti operasi penjumlahan, perlu diperhatikan pangkat polinomialnya. Jika mengurangkan suku yang sejenis, misalkan

$$f(x) = 6x^2 - 2x^2 = 4x^2$$

Sedangkan jika menjumlahkan suku yang berbeda, misalkan $6x^3$ dan $2x^2$ maka diperoleh $6x^3 - 2x^2$.

3. Perkalian

Operasi perkalian pada polinomial mempunyai sifat distributif yaitu:

$$a * (b + c) = a * b + a * c$$

$$(a + b)(c + d) = ac + ad + bc + bd$$

Dimana a, b, c dan d adalah koefisien dari polinomial. sifat distributif pada perkalian polinomial ini juga berlaku untuk operasi penjumlahan dan operasi pengurangan. Proses perkalian antara fungsi polinomial $f(x)$ dan fungsi polinomial $h(x)$ melibatkan perkalian masing-masing suku dari kedua fungsi polinomial tersebut.

4. Pembagian

Pembagian dalam operasi polinomial umumnya dilakukan dengan metode susun dan horner. Dengan menerapkan metode ini, kita dapat mengidentifikasi hasil bagi dan sisa pada operasi pembagian polinomial. Definisi pembagi pada polinomial dapat ditulis sebagai berikut:

$$p(x) = q(x).h(x) + s(x)$$

Keterangan:

$p(x)$ = Polinomial yang akan dibagi

$q(x)$ = Pembagi polinomial

$h(x)$ = Hasil bagi

$s(x)$ = Sisa pembagian

2.2.3 Lapangan Hingga dengan Elemen Polinomial $GF(2^n)$

Lapangan hingga dengan struktur paling sederhana yaitu lapangan hingga yang nilai order nya merupakan bilangan prima, yang dinotasikan dengan $GF(p)$. Selain itu pada sistem kriptografi, Galois field yang umumnya digunakan adalah $GF(p^n)$, dimana $GF(p^n)$ berasal dari aritmetika modular polinomial $m(x)$ yang ditulis sebagai berikut:

$$m(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \alpha_{n-2} x^{n-2} + \cdots + \alpha_1 x^0 + x_0$$

Polinomial $m(x)$ merupakan polinomial berderajat n dengan koefisien yang berasal dari elemen-elemen didalam $GF(p^n)$. Polinomial $m(x)$ dikenal sebagai polinomial tak tereduksi. Karakteristik polinomial tak tereduksi $m(x)$ mirip dengan bilangan prima, yaitu tidak habis dibagi kecuali oleh dirinya sendiri dan (Sadikin , 2012).

Definisi Suatu polinomial pada $GF(p^n)$ disebut tak tereduksi jika polinomial tersebut tidak habis dibagi oleh polinomial manapun pada $GF(p^n)$ yang derajatnya lebih kecil.

Elemen pada $GF(p^n)$ merupakan semua polinomial yang berderajat antara 0 sampai $n - 1$ dengan koefisien yang merupakan elemen pada $GF(p)$. Misalnya elemen pada $GF(p^n)$ ditulis sebagai $f(x)$, maka

$$f(x) = \alpha_{n-1} x^{n-1} + \alpha_{n-2} x^{n-2} + \cdots + \alpha_1 x^0 + x_0$$

Dengan $\alpha_i \in GF(p^n)$ dan $\alpha_n \neq 0$.

2.2.4 Aritmatika Modulo Polinomial

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 $GF(2^n)$

\times	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).

2.3 Kode Linier

Kode linier adalah kode koreksi kesalahan yang setiap kombinasi linier dari kata kode. Kode linear seringkali didefinisikan dalam konteks ruang vektor atas sebuah bidang tertentu, biasanya pada medan \mathbb{F}_2 . sebuah kode linear atas medan

\mathbb{F}_2 adalah subruang dari \mathbb{F}_2^n , diaman \mathbb{F}_2 adalah medan biner yang terdiri dari elemen 0 dan 1, dan n adalah panjang vektor dalam kode tersebut.

Definisi Kode linier berdimensi k dan panjang n pada suatu bidang \mathbb{F} adalah subruang berdimensi k dari ruang vektor \mathbb{F}^n , himpunan vektor bedimensi n dan dapat disebut sebagai kode $[n, k]$ jika jarak Hamming Minimum dari kode tersebut adalah d , maka kode tersebut kode $[n, k, d]$ (Ling & Xing, 2004).

2.4 Matriks Generator dan Matriks Parity Check

Definisi Matriks $G = (I_k, A^T)$ disebut matriks generator atau matriks encoding dari kode linear (n, k) dengan matriks cek paritas $H = (-A, I_{n-k})$ pada bentuk baku. Jelas didapatkan $GH^T = 0$ (Ling & Xing, 2004).

Teorema Jika C adalah (n, k) -code atas F , maka C^\perp adalah $(n, n - k)$ -code atas F . Dari teorema diatas dapat disimpulkan bahwa: jika $G = (I_k, A^T)$ adalah matriks generator untuk C , maka $H = (-A, I_{n-k})$ adalah matriks generator untuk C^\perp .

Contoh

Misalkan C adalah $(6, 3)$ -code atas Z_2 yang dibangun oleh $G_1 =$

$\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$, kemudian dengan operasi baris elementer diperoleh

matriks generator

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} = [I_3, A]$$

Dengan $A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$. Selanjutnya matriks generator untuk C^\perp adalah

$$H = (-A^T, I_3) = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Matriks G dan H tersebut memenuhi $GH^T = 0$.

2.5 Kode Goppa

Kode goppa merupakan kode linier yang mengoreksi kesalahan yang dapat digunakan untuk mengenkripsi dan mendekripsi pesan.

Definisi Misalkan polinomial Goppa didefinisikan sebagai polinomial pada $GF(2^m)$, yaitu

$$g(x) = g_0 + g_1x + \dots + g_t x^t = \sum_{i=0}^t g_i x^i$$

Dengan masing-masing $g_i \in GF(2^m)$. Dan himpunan lokasi L merupakan himpunan elemen-elemen dari bidang *eksistensi* $GF(2^m)$.

$$L = \{\alpha_1, \dots, \alpha_n\} \subseteq GF(2^m)$$

Sehingga $g(\alpha_i) \neq 0$ untuk semua $\alpha_i \in L$. Untuk vektor *codeword* $c = (c_1, \dots, c_n)$ pada $GF(2^m)$, maka kita mempunyai fungsi berikut

$$R_c(x) = \sum_{i=1}^n \frac{c_i}{x - \alpha_i}$$

di mana $\frac{1}{x - \alpha_i}$ adalah suatu polinomial yang unik dengan $(x - \alpha_i) \cdot \frac{1}{x - \alpha_i} \equiv 1 \pmod{g(x)}$ dengan derajat kurang dari sama dengan $t - 1$. Kemudian, kode Goppa $\Gamma(L, g(x))$ yang terdiri dari semua vektor kode c sedemikian rupa sehingga $R_c(x) \equiv 0 \pmod{g(x)}$ di mana polinomial $g(x)$ membagi $R_c(x)$ (Ling & Xing, 2004).

Definisi Untuk polinomial Goppa $g(x)$ berderajat t dan $L = \{\alpha_1, \dots, \alpha_n\}$, kode Goppa $\Gamma(L, g(x))$ adalah kode linier atas $GF(q)$ dengan parameter $[n, k, d]$, dimana $k \geq n - mt$ dan $d \geq t + 1$ (Ling & Xing, 2004).

Ingatlah bahwa Kode Goppa adalah kode linier, oleh karena itu dapat dinotasikan dengan $[n, k, d]$ untuk mendeskripsikan kode goppa dengan panjang parameter n , dimensi k , dan jarak *hamming* minimum d . Panjang n hanya bergantung pada subset L .

Definisi *Parity check matrix* pada kode Goppa didefinisikan sebagai matrix H sehingga $Hc^T = 0$ untuk semua vektor kode c dalam $GF(p^m)$ yang memenuhi syarat kode Goppa.

$$H = \begin{pmatrix} (g_t \alpha_1 + g_{t-1})g(\alpha_1)^{-1} & (g_t \alpha_2 + g_{t-1})g(\alpha_2)^{-1} & \cdots & (g_t \alpha_n + g_{t-1})g(\alpha_n)^{-1} \\ g_t g(\alpha_1)^{-1} & g_t g(\alpha_2)^{-1} & \cdots & g_t g(\alpha_n)^{-1} \end{pmatrix}$$

2.6 Algoritma Petterson

Algoritma petterson hanya digunakan untuk decoding kode goppa. Dengan menghitung sindrom $s(x)$ dari vektor yang diterima dan kemudian menyelesaikan persamaan kunci $\sigma(z)s(x) \equiv w(z) \text{ mod } g(z)$ dengan $w(z) = \sigma'(z)$. Polinomial untuk mencari kesalahan dapat dibagi menjadi pangkat genap dan pangkat ganjil dari z . Algoritma petterson dapat digambarkan sebagai berikut (Singh, 2020) :

1. Menghitung *syndrome*

$$s(x) \equiv \sum_{i=1}^n \frac{y_i}{x - \alpha_i}$$

2. Selesaikan persamaan kunci

$$\sigma(x)s(x) \equiv \sigma'(x) \text{ mod } g(x)$$

3. Tentukan himpunan lokasi error $B = \{i | \sigma(\alpha_i) = 0\}$.
4. Tentukan vektor *error* $e = (e_1, \dots, e_n)$, dengan $e_i = 1$ untuk $i \in B$ dan $e_i = 0$ ditempat yang lain.
5. Hitung *codeword* $\hat{m} = y - e$.

2.7 Kriptografi

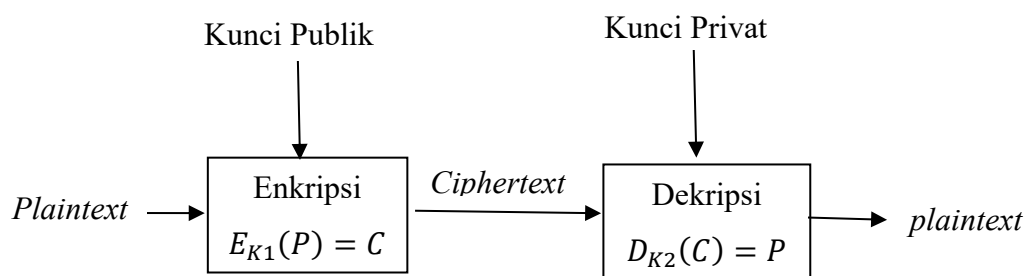
Kata kriptografi berasal dari bahasa Yunani dimana '*Cryptos*' memiliki arti tersembunyi dan '*Graphein*' berarti tulisan. Menurut Bruce Schneier, kriptografi adalah ilmu pengetahuan dan seni menjaga pesan agar aman (*secure*) (Rosdiana, 2015). Meskipun sangat sederhana, konsep kriptografi sendiri telah lama digunakan oleh manusia, seperti pada peradaban Mesir dan Romawi. Seiring dengan berkembangnya teknologi, tuntutan keamanan terhadap kerahasiaan informasi semakin meningkat.

Terdapat dua teknik utama dalam kriptografi yaitu enkripsi dan dekripsi. Enkripsi adalah teknik dimana pesan asli (*plaintext*) yang akan dikirim diubah menjadi pesan acak (*ciphertext*) dengan menggunakan algoritma tertentu. Dekripsi merupakan teknik untuk mengembalikan pesan acak menjadi pesan asli. Proses enkripsi dan dekripsi ini dapat mengurangi dampak dibobolnya pesan oleh pihak yang tidak berhak.

Kriptografi membentuk sebuah sistem yang disebut sebagai sistem kriptografi (*cryptosystem*), dimana suatu *cryptosystem* terdiri dari *plaintext*, *ciphertext*, kunci dan algoritma kriptografi. Algoritma kriptografi merupakan langkah-langkah yang disusun secara sistematis dan logis yang digunakan untuk menyembunyikan pesan. Dengan adanya algoritma kriptografi proses enkripsi akan lebih mudah. Algoritma kriptografi berdasarkan jenis kuncinya dibagi menjadi dua yaitu kriptografi kunci simetri dan kriptografi kunci asimetri.

2.8 Sistem Kriptografi Kunci Publik

Kriptografi kunci asimetri adalah algoritma dimana kunci yang digunakan pada saat proses enkripsi berbeda dengan kunci pada dekripsi. Kriptografi kunci asimetri ini disebut juga sebagai kriptografi kunci publik (*public-key cryptography*). Kunci pada proses enkripsi ini disebut kunci publik (*public key*) yaitu dapat diketahui oleh siapapun yang tidak mempunyai otoritas pesan tersebut, sedangkan kunci pada proses dekripsi disebut kunci privat/pribadi (*private key*) sehingga kunci ini tidak disebar dan hanya digunakan oleh pengirim pesan. Skema kriptografi kunci publik sebagai berikut (Surnawani, Jarkasih, & Fatimah, 2022):



Gambar 2.1 Skema Kriptografi Kunci Publik

2.9 Kriptosistem McEliece

Pada tahun 1987 Robert J. McEliece memperkenalkan kriptosistem McEliece sebagai kriptosistem pertama yang menggunakan kode *error-correcting*, dengan sistem keamanan yang bergantung pada kesulitan decoding disertai *error* yang acak. Kriptosistem *McEliece* adalah jenis kriptosistem kunci publik yang menggunakan kode linier yang mengoreksi kesalahan untuk membuat kunci publik dan kunci privat. Kode koreksi kesalahan yang digunakan dalam kriptosistem ini adalah kode *Goppa Binary*. Nilai n , k dan t adalah parameter yang tersedia untuk

umum, tetapi L, g, P dan S adalah rahasia yang dihasilkan secara acak (Singh, 2020). Kriptosistem ini memiliki tiga tahapan mekanisme. Tahapan pertama yaitu pembangkitan kunci, tahap kedua yaitu enkripsi, dan ketiga yaitu tahap dekripsi.

2.9.1 Pembangkitan Kunci

Menghitung matriks generator G berukuran $k \times n$ yang dibangkitkan sesuai dengan parameter kode yang digunakan. Selanjutnya menentukan matriks random S berukuran $k \times k$ yang berguna untuk mengacak susunan matriks generator kode agar tersembunyi. Dan menentukan matriks permutasi P berukuran $n \times n$ yang dibangun secara acak sehingga mengaburkan elemen pada matriks generator. Kemudian pembangkitan kunci publik diperoleh dari hasil perkalian matriks-matriks G, P dan S sebagai berikut:

$$G' = SGP$$

Keterangan:

G' = Kunci Publik

k = Dimensi

n = Panjang

Dari perhitungan di atas, diperoleh dua pasang kunci yaitu kunci publik (G'), dan kunci privat yaitu G, P dan S .

2.9.2 Proses Enkripsi

Langkah pertama pada proses enkripsi adalah menerjemahkan pesan ke dalam kode ASCII. Selanjutnya nyatakan pesan sebagai bilangan m , bagi pesan ke dalam blok-blok dengan panjang yang sesuai dengan ukuran dimensi (k).

Notasikan blok pesan dengan $m = m_1, m_2, \dots, m_k$. Berikut langkah-langkah enkripsi:

1. Pengirim memilih vektor biner secara acak dengan panjang n dan bobot t .

Dan notasikan vektor ini dengan e .

2. Pengirim mengenkripsi pesan m menjadi y dengan persamaan

$$C' = mG' + e$$

Pesan y adalah pesan yang telah dienkripsi.

2.9.3 Proses Dekripsi

Setelah pesan C' diterima, lakukan proses dekripsi dengan langkah-langkah berikut:

1. Hitung $Y = C'P^{-1}$, dengan P^{-1} adalah invers dari matriks permutasi P .
2. Gunakan algoritma decoding pada Y sehingga diperoleh $\hat{m} = mS$.
3. Kalikan \hat{m} dengan S^{-1} sehingga diperoleh $m = \hat{m}S^{-1}$.
4. Gabungkan semua blok-blok m , lalu ubah m ke dalam bentuk alfabet biasa untuk mendapatkan pesan asli.

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

Al-Qur'an adalah wahyu Allah SWT yang diberikan kepada Rasulullah SAW sebagai pedoman bagi umat islam. Al-qur'an tidak hanya mencakup tentang ayat-ayat yang berkaitan dengan kepercayaan dan hukum syariah, tetapi juga mencakup isu-isu yang berkaitan dengan perilaku manusia, baik yang diperintahkan maupun yang dilarang (Andika, Taquyuddin, & Admizal, 2020). Salah satu contohnya adalah perintah untuk menjadi amanah dan melakukan kebenaran, baik itu jenis

kebenaran yang berhubungan dengan Allah maupun sesama manusia dan diri sendiri. Hal ini seperti yang telah dijelaskan dalam Firman Allah mengenai pentingnya menjaga amanat dalam Q.S An-Nisa' ayat 58:

﴿ إِنَّ اللَّهَ يَأْمُرُكُمْ أَنْ تُؤَدُّوا الْأَمَانَاتِ إِلَىٰ أَهْلِهَا وَإِذَا حَكَمْتُمْ بَيْنَ النَّاسِ أَنْ تَحْكُمُوا بِالْعَدْلِ ۗ ﴾

﴿ إِنَّ اللَّهَ نِعِمَّا يَعِظُكُمْ بِهِ ۗ إِنَّ اللَّهَ كَانَ سَمِيعًا بَصِيرًا ﴾

Artinya: “*Sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya, dan (menyuruh kamu) apabila menetapkan hukum di antara manusia supaya kamu menetapkan dengan adil. Sesungguhnya Allah memberi pengajaran yang sebaik-baiknya kepadamu. Sesungguhnya Allah adalah Maha Mendengar lagi Maha Melihat*” (Q.S An-Nisa' :58)

Berdasarkan ayat diatas, dijelaskan bahwa amanah merupakan sesuatu yang diserahkan kepada pihak lain untuk dijaga dan dikembalikan ketika diminta oleh pemiliknya. Kita diperintahkan untuk menyampaikan amanah dan ditekankan bahwa amanah tersebut harus disampaikan kepada pemiliknya. Menurut Darimis amanah mempunyai arti benar-benar bisa dipercaya. Artinya adalah bahwa seseorang yang diberi sebuah amanah harus menjalankannya dengan sungguh-sungguh dan sesuai dengan apa yang diberikan. Dengan melakukan hal tersebut, orang yang memberi amanah akan memiliki kepercayaan kepada kita tanpa perlu penjelasan apapun (Sahri, 2018).

Seruan Al-Qur'an mengenai amanah tidak hanya berkaitan dengan kepercayaan dan tanggung jawab seseorang, tetapi juga berhubungan dengan tingkat keimanan seseorang. Disebutkan bahwa individu yang memiliki keimanan seharusnya juga memiliki sifat amanah, yang dianggap sebagai sifat terpuji dan juga sifat kenabian. Amanah merupakan salah satu karakteristik yang harus dimiliki oleh nabi saat menjalankan tugas-tugasnya untuk menyampaikan kebenaran yang

berasal dari Allah SWT. Seperti contoh, saat kaum nabi Nuh a.s melakukan penolakan terhadap Allah SWT, turunlah firman Allah SWT untuk menegaskan bahwa nabi Nuh a.s adalah orang yang dapat dipercaya melalui Al-Qur'an surah Asy-Syu'ara ayat 105-107:

كَذَّبَتْ قَوْمُ نُوحٍ الْمُرْسَلِينَ ﴿١٠٥﴾ إِذْ قَالَ لَهُمْ أَخُوهُمْ نُوحٌ أَلَا تَتَّقُونَ ﴿١٠٦﴾ إِنِّي لَكُمْ رَسُولٌ أَمِينٌ ﴿١٠٧﴾

Artinya: “Kaum Nuh telah mendustakan para rasul. Ketika saudara mereka (Nuh) berkata kepada mereka, Mengapa kamu tidak bertakwa?, Sesungguhnya aku adalah seorang rasul terpercaya (yang diutus) kepadamu.”

Dalam konteks kenabian, sifat amanah ini menjadi kualitas utama yang memastikan bahwa seorang rasul dapat dapat dipercaya untuk menyampaikan wahyu dan petunjuk dari Allah SWT kepada umatnya. Islam mengajarkan bahwa amanah merupakan asas dari keimanan seperti sabda Nabi SAW :

عَنْ أَنَسٍ قَالَ مَا خَطَبَنَا رَسُولُ اللَّهِ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ إِلَّا قَالَ لَا إِيمَانَ لِمَنْ لَا أَمَانَةَ لَهُ
وَلَا دِينَ لِمَنْ لَا عَهْدَ لَهُ (رواه الطبراني)

Artinya: Dari Anas, ia berkata Rosulullah SAW tidak berkhotbah kecuali bersabda: Tidak ada keimanan bagi orang yang tidak melaksanakan amanah, dan tidak ada agama bagi orang yang tidak menepati janji.(H.R al-Thabarani)

Hadist ini menyampaikan, bahwa keimanan seseorang tidak akan mencapai tingkat kesempurnaan jika dia tidak memenuhi kewajiban amanah dan menepati janjinya. Bagi seorang muslim, keimanan akan mendatangkan ketakwaan. Karena ketakwaan akan mendorongnya untuk selalu berhati-hati terhadap segala hal yang dapat membahayakan dirinya. Salah satu perintah yang harus dijalankan oleh

seorang yang beriman adalah menjalankan amanah dengan penuh tanggung jawab (Halim & Zulheldi, 2019).

Secara khusus, amanah dapat merujuk pada tindakan menjaga dan mengembalikan sesuatu yang dipercayakan kepada pemiliknya dalam keadaan semula. Sementara itu dalam arti yang lebih umum, amanah melibatkan sejumlah aspek, seperti merahasiakan informasi orang lain, menjaga reputasi orang lain, menjaga diri sendiri dan menunaikan tugas-tugas yang diberikan. Tugas-tugas yang Allah SWT berikan kepada manusia itu merupakan amanah yang paling berat dan besar atau disebut amanah *taklif* (Abidin & Khairudin, 2017). Karena amanah yang diberikan Allah kepada manusia begitu besar, bahkan diilustrasikan bahwa langit, bumi dan gunung tidak akan mampu mengemban amanah tersebut. Seperti yang dijelaskan dalam al-qu'an surah Al-Ahzab ayat 72 (Kemenag RI, 2024):

إِنَّا عَرَضْنَا الْأَمَانَةَ عَلَى السَّمَوَاتِ وَالْأَرْضِ وَالْجِبَالِ فَأَبَيْنَ أَنْ يَحْمِلْنَهَا وَأَشْفَقْنَ مِنْهَا
وَحَمَلَهَا الْإِنْسَانُ إِنَّهُ كَانَ ظَلُومًا جَهُولًا

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*”.

Menurut Muhammad Nassib Ar-Rifa'i dalam Buku Ringkasan Ibnu Katsir jilid 4, dijelaskan bahwa karakteristik orang yang dapat dipercaya terletak pada kemampuannya untuk memelihara amanah dan menjaga janjinya. Mereka yang memiliki sifat beriman tidak akan mengkhianati amanah yang diberikan kepada mereka dan selalu memenuhi janji yang diucapkan. Allah SWT melarang umatnya untuk tidak mengkhianati amanah, karena amanat memiliki hubungan erat dengan

kepercayaan. Jika amanah tidak dijaga dengan baik maka kepercayaan akan hilang, sehingga dapat mengakibatkan ketenangan hidup dalam kehidupan bermasyarakat. Sebaliknya, perbuatan khianat merupakan tindakan yang bertentangan dengan sifat amanah. Khianat menjadi ciri khas orang munafik yang dapat merusak iman seorang mukmin. Dalam sebuah hadits yang diriwayatkan oleh Imam Bukhari (Al Albani, 2007), disebutkan tiga tanda orang munafik:

عَنْ أَبِي هُرَيْرَةَ عَنِ النَّبِيِّ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ قَالَ: آيَةُ الْمُنَافِقِ ثَلَاثٌ إِذَا حَدَّثَ كَذَبَ
وَإِذَا وَعَدَ أَخْلَفَ وَإِذَا أُؤْتِمِنَ خَانَ (رواه البخاري)

Artinya: *Dari Abu Hurairah r.a., dari Rasulullah SAW bersabda: "Tanda-tanda munafik ada 3 yaitu jika berbicara dusta, jika berjanji mengingkari, dan jika diberi amanah dia khianat"*

Selanjutnya, Allah SWT berfirman :

يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَخُونُوا اللَّهَ وَالرَّسُولَ وَتَخُونُوا أَمْنَتِكُمْ وَأَنْتُمْ تَعْلَمُونَ ﴿٢٧﴾

Artinya: *"Wahai orang-orang yang beriman, janganlah kamu mengkhianati Allah dan Rasul serta janganlah kamu mengkhianati amanat yang dipercayakan kepadamu, sedangkan kamu mengetahui".(Q.S Al-Anfal:27)*

Ayat ini menekankan pentingnya untuk tidak melakukan pengkhianatan terhadap Allah SWT, Rasul-Nya, dan amanah-amanah yang dipercayakan, dapat dihubungkan dengan konsep kriptografi dalam konteks keamanan pesan. Sama seperti ayat yang menyoroti pentingnya mempertahankan kepercayaan dan menghindari pengkhianatan dalam konteks sosial, kriptografi berfungsi sebagai sarana untuk mengamankan dan melindungi informasi di ranah digital.

Pada zaman Rasulullah SAW dan peperangan pada masa itu, penyampaian pesan rahasia memerlukan kecerdikan dan strategi tertentu. Rasulullah SAW

memanfaatkan intelijen dan informan yang dapat menyampaikan pesan rahasia tentang rencana musuh atau pergerakan pasukan mereka. Dalam sejarah islam, Hudzaifah bin Al-Yaman merupakan seorang kepercayaan Rasulullah SAW untuk mematai rencana kaum kafir dan orang munafik, khususnya dalam perang khandaq. Dengan mengumpulkan informasi secara diam-diam, Rasulullah dan para sahabatnya dapat membuat keputusan yang lebih bijaksana dan efektif di medan perang.

Di zaman modern ini, kepercayaan dan keamanan sangat penting, terutama dalam pengiriman informasi yang bersifat sensitif. Kriptografi, yang melibatkan pengkodean dan dekoding pesan untuk melindunginya dari akses yang tidak sah, merupakan salah satu komitmen di zaman modern ini untuk mempertahankan kepercayaan dan mencegah pengkhianatan dalam komunikasi. Sebagaimana pengkhianatan kepercayaan dalam konteks sosial dapat menyebabkan ketidakstabilan dan ketidakamanan dalam masyarakat, pelanggaran keamanan kriptografi dapat mengakibatkan data terancam, kehilangan privasi, dan bahaya potensial bagi individu atau masyarakat.

Oleh karena itu, pesan mendasar dari ayat Al-Qur'an yang mendorong integritas terkait dengan prinsip-prinsip keamanan informasi yang diterapkan dalam ilmu kriptografi. Keduanya menekankan pentingnya menjaga kepercayaan dan memastikan stabilitas serta keamanan dalam bidangnya masing-masing. Baik dalam konteks kehidupan yang ditonjolkan dalam ayat atau dalam ranah digital di mana kriptografi memainkan peran penting dalam mengamankan komunikasi dan menjaga kerahasiaan.

2.11 Kajian Topik dengan Teori Pendukung

Salah satu dampak besar terhadap kehidupan muncul seiring dengan kemajuan teknologi informasi yang pesat. Meskipun memberikan kemudahan dalam menyebarkan informasi, perkembangan ini juga menyebabkan peningkatan kasus kejahatan yang berasal dari internet, yang mengakibatkan ketidakamanan pengguna internet saat melakukan pengiriman pesan. Oleh karena itu, untuk mengatasi ketakutan akan kebocoran pesan, perlu diterapkan ilmu kriptografi sebagai keamanan pesan. Dengan menggunakan kriptografi, dapat meminimalkan resiko kebocoran informasi oleh pihak yang tidak berwenang.

Penelitian ini membahas mengenai sistem kriptografi yang aman terhadap serangan *post quantum*. Digunakanlah kriptosistem McEliece untuk menciptakan sistem keamanan yang baik. Kriptosistem McEliece ini adalah salah satu bentuk enkripsi kunci publik yang mengandalkan kesulitan dalam mendekripsikan informasi tanpa kunci privat yang sesuai. Untuk menambah kekuatan pada kunci McEliece, digunakan implementasi kode Goppa agar tingkat keamanan lebih kuat. Dalam hal ini, kode Goppa yang berasal dari teori pengkodean digunakan sebagai bagian dari skema keamanan McEliece. Kode Goppa memanfaatkan polinomial untuk membentuk matriks generator yang kompleks. Konsep teori bilangan juga diterapkan untuk mengoptimalkan pemilihan parameter dan parameter kunci.

BAB III

METODE PENELITIAN

3.1 Jenis Penelitian

Penelitian ini termasuk jenis penelitian kualitatif, dimana penelitian diambil dari sebuah data yang kemudian memanfaatkan teori yang ada sebagai bahan untuk penjas. Metode penelitian yang digunakan adalah studi literatur yang bertujuan untuk mengembangkan aspek teoritis. Metode ini sangat berguna untuk mengidentifikasi pengetahuan yang belum diketahui, mengembangkan teori baru, atau merancang kerangka dasar untuk penelitian lebih lanjut dalam berbagai bidang ilmu pengetahuan. Dengan demikian, penelitian ini memungkinkan peneliti untuk memahami suatu masalah atau fenomena hanya dengan menganalisis dari buku atau jurnal.

3.2 Pra Penelitian

Proses pra penelitian ini diawali dengan melakukan tinjauan literatur yang komprehensif untuk memahami penelitian yang telah dilakukan sebelumnya. Tinjau artikel jurnal, buku, laporan penelitian, atau sumber informasi lain yang relevan dengan penelitian terkait. Selain itu penulis juga mempelajari bagaimana cara untuk memodifikasi pembangkit kunci pada kriptosistem McEliece. Kemudian mengidentifikasi kekurangan dan kelebihan metode yang akan digunakan.

3.3 Tahapan Penelitian

1. Pembangkitan Kunci

- a. Pilih polinomial $g(x)$ dengan derajat t atas $GF(2^4)$ dengan parameter $[n, k, d]$, di mana n merupakan panjang parameter kode dan k merupakan dimensi kode yang mampu memperbaiki t error dan d merupakan jarak minimum kode.
- b. Menentukan matriks generator berukuran $k \times n$ yang dibangkitkan berdasarkan parameter kode Goppa.
- c. Menentukan matriks permutasi P berukuran $n \times n$, di mana P adalah matriks yang memuat 1 pada setiap baris dan setiap kolom.
- d. Menentukan secara acak matriks S berukuran $k \times k$ yang merupakan matriks non-singular.
- e. Kemudian menghitung G' dengan ukuran $k \times n$ sebagai kunci publik.

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

2. Proses Enkripsi pada Kriptosistem McEliece

- a. Menentukan pesan sebagai *plaintext*, kemudian mengubah ke bentuk binary berdasarkan tabel ASCII sebagai *binary string* m dengan panjang k .
- b. Pesan m dikalikan dengan kunci publik G' .
- c. Menentukan vektor *error* e berukuran n -bit yang mengandung t (vektor dengan panjang n dan bobot t).
- d. Menambahkan kesalahan pada *codeword* $C'_i = C_i + e$.

3. Proses dekripsi pada Kriptosistem McEliece

- a. Menghitung invers dari matriks P .

- b. Menghitung $Y_i = C_i' \times P^{-1}$.
- c. Menggunakan algoritma decoding sehingga diperoleh \hat{m} .
- d. Menghitung $m = \hat{m}S^{-1}$.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Pembentukan Kunci

Algoritma pembentukan kunci dalam kriptosistem McEliece memiliki peran penting untuk menjamin keamanan dan efektivitas sistem ini. proses ini dimulai dari penentuan nilai n dan k yang digunakan untuk pembentukan matriks generator G , dimana n merupakan panjang suatu kode atau jumlah kolom dalam matriks generator G , dan k merupakan dimensi kode atau jumlah baris dalam matriks generator G . Keistimewaan algoritma McEliece terletak pada penggunaan matriks permutasi acak P dan matriks S yang dihasilkan secara acak untuk pembentukan kunci publik. Proses ini memiliki kerumitan struktural yang meningkat keamanan kunci publik, menjadikan algoritma McEliece sebagai pendekatan yang kuat dalam melindungi pesan dari serangan terhadap sistem kriptografi.

4.1.1 Algoritma Pembentukan Kunci pada Kriptosistem McEliece

1. Input:
 - a. Menentukan nilai n dan k sesuai dengan polinomial kode Goppa sebagai parameter kode.
 - b. Bangkitkan matriks generator G dengan ukuran $n \times k$.
 - c. Bangkitkan matriks random S berukuran $k \times k$ yang merupakan matriks non-singular.
 - d. Bangkitkan matriks random P berukuran $n \times n$ yang merupakan matriks permutasi.

2. Proses:

Hitung matriks G' menggunakan rumus berikut:

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

3. Output:

Matriks G' merupakan kunci publik yang akan digunakan sebagai matriks generator pada tahap enkripsi. Matriks S , G dan P sebagai kunci privat.

4.1.2 Simulasi Pembentukan Kunci pada Kriptosistem McEliece

Misalkan dipilih lapangan hingga $GF(2^4) = \{0, 1, \alpha, \alpha^2, \dots, \alpha^{14}\}$ dengan α elemen primitif yang memenuhi $\alpha^4 + \alpha + 1 = 0$. Sehingga diperoleh nilai elemen untuk $GF(2^4)$ sebagai berikut:

Tabel 4.1 Representasi Polinomial $GF(2^4)$

α_i	Representasi Polinomial
0	= 0
α^0	= 1
α^1	= α
α^2	= α^2
α^3	= α^3
α^4	= $1 + \alpha$
α^5	= $\alpha + \alpha^2$
α^6	= $\alpha^2 + \alpha^3$
α^7	= $1 + \alpha + \alpha^3$
α^8	= $1 + \alpha^2$

α^9	$= \alpha + \alpha^3$
α^{10}	$= 1 + \alpha + \alpha^2$
α^{11}	$= \alpha + \alpha^2 + \alpha^3$
α^{12}	$= 1 + \alpha + \alpha^2 + \alpha^3$
α^{13}	$= 1 + \alpha^2 + \alpha^3$
α^{14}	$= 1 + \alpha^3$

(Sumber : Singh, 2020)

Didefinisikan kode Goppa $\Gamma(L, g(x))$ dengan pilihan polinomial berikut:

$$g(x) = (x + \alpha)(x + \alpha^{14}) = x^2 + \alpha^7x + 1,$$

$$L = \{\alpha^i | 2 \leq i \leq 13\}$$

Untuk kode ini, $m = 4$, $n = 12$ dan $t = 2$. Maka kita dapatkan $k \geq 12 - 4 \cdot 2 = 4$ dan $d \geq 2 \cdot 2 + 1 = 5$. Jadi kode ini adalah kode Goppa $[12, \geq 4, \geq 5]$. Menentukan parameter kunci n dan k , dimana berdasarkan kode Goppa diketahui bahwa nilai $n = 12$ dan $k \geq 4$. Selanjutnya matriks generator G ditentukan dengan menggunakan aplikasi *sagemath* sebagai berikut:

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

Berdasarkan generator matriks yang telah diperoleh diatas dimensi matriks ini adalah 4×12 maka dapat disimpulkan bahwa kode Goppa $\Gamma(L, g(x))$ berdimensi 4, sehingga parameternya $[12, 4, \geq 5]$. Selanjutnya, dilakukan pembangkitan matriks S secara acak dengan dimensi $k \times k$ dan matriks P dengan dimensi $n \times n$ menggunakan aplikasi *sagemath*.

Dengan demikian, kita dapatkan matriks G' dengan ukuran 12×4 yang siap digunakan sebagai kunci publik pada tahap enkripsi dalam algoritma McEliece.

4.2 Proses Enkripsi

Enkripsi pada kriptosistem mceliece melibatkan penggunaan kode-kode koreksi error untuk menyembunyikan informasi rahasia. Proses enkripsi dimulai dengan pemilihan pesan plaintext yang akan dienkripsi. Pesan ini kemudian diubah menjadi vektor biner yang panjangnya sesuai dengan dimensi kode, yaitu k . Vektor biner ini kemudian dikalikan dengan kunci publik G' . Hasil dari perkalian ini merupakan sebuah vektor *ciphertext* yang kemudian ditambahkan dengan vektor *error* acak e . Vektor error ini menambahkan kerumitan yang membuat dekripsi oleh pihak yang tidak berwenang menjadi sangat sulit.

4.2.1 Algoritma Enkripsi Menggunakan McEliece

1. Input:
 - a. Menentukan plainteks yang akan dikirimkan.
 - b. Menentukan vektor e dengan panjang n dan bobot t .
2. Proses:
 - a. Mengubah plainteks ke bentuk binary berdasarkan tabel ASCII dan notasikan sebagai m .
 - b. Membagi dalam blok-blok dengan panjang 4 bit.
 - c. Hitung vektor $C_i = m \times G'$
 - d. Hitung $C'_i = C_i + e$

3. Output:

Matriks C' merupakan *ciphertext* yang siap untuk dikirimkan.

4.2.2 Simulasi Proses Enkripsi Menggunakan Algoritma McEliece

Sebagai contoh pengirim akan mengirimkan pesan KAMU, berdasarkan tabel ASCII pesan KAMU direpresentasikan dalam bentuk biner yaitu 01001011010000010100110101010101. Sehingga, vektor dari masing-masing karakter hurufnya adalah sebagai berikut:

$$K = [0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1]$$

$$A = [0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1]$$

$$M = [0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1]$$

$$U = [0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1]$$

Kemudian membagi kode biner ke beberapa blok m_i dengan panjang 4 bit berdasarkan dimensi k pada parameter kode Goppa.

$$m_1 = [0 \ 1 \ 0 \ 0]$$

$$m_2 = [1 \ 0 \ 1 \ 1]$$

$$m_3 = [0 \ 1 \ 0 \ 0]$$

$$m_4 = [0 \ 0 \ 0 \ 1]$$

$$m_5 = [0 \ 1 \ 0 \ 0]$$

$$m_6 = [1 \ 1 \ 0 \ 1]$$

$$m_7 = [0 \ 1 \ 0 \ 1]$$

$$m_8 = [0 \ 1 \ 0 \ 1]$$

Selanjutnya pesan m_i yang telah diubah ke bentuk biner dikalikan dengan kunci publik G' untuk menghasilkan matriks C_i .

$$\begin{aligned}
C_6 &= m_6 \times G' = [1 \ 1 \ 0 \ 1] \\
&\quad \times \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \\
&= [1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0]
\end{aligned}$$

$$\begin{aligned}
C_7 &= m_7 \times G' = [0 \ 1 \ 0 \ 1] \\
&\quad \times \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \\
&= [1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1]
\end{aligned}$$

$$\begin{aligned}
C_8 &= m_8 \times G' = [0 \ 1 \ 0 \ 1] \\
&\quad \times \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \\
&= [1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1]
\end{aligned}$$

Kemudian C_i ditambahkan dengan *error* acak e dengan panjang 12 bit berdasarkan panjang n pada parameter kode Goppa, dalam hal ini $e = [0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1]$. Dan didapatkan nilai C'_i sebagai berikut:

$$\begin{aligned}
C'_1 &= C_1 + e = [1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 0] \\
&\quad + [0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1] \\
&= [1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1]
\end{aligned}$$

$$\begin{aligned}
C'_2 &= C_2 + e = [1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1] \\
&\quad + [0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1] \\
&= [1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0]
\end{aligned}$$

$$\begin{aligned}
C'_3 &= C_3 + e = [1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 0] \\
&\quad + [0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1] \\
&= [1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1]
\end{aligned}$$

$$\begin{aligned}
C'_4 &= C_4 + e = [0 \ 1 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1] \\
&\quad + [0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1] \\
&= [0 \ 1 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 0]
\end{aligned}$$

$$\begin{aligned}
C'_5 &= C_5 + e = [1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 0] \\
&\quad + [0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1] \\
&= [1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1]
\end{aligned}$$

$$\begin{aligned}
C'_6 &= C_6 + e = [1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0] \\
&\quad + [0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1] \\
&= [1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1]
\end{aligned}$$

$$\begin{aligned}
C'_7 &= C_7 + e = [1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1] \\
&\quad + [0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1] \\
&= [1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0]
\end{aligned}$$

$$\begin{aligned}
C'_8 &= C_8 + e = [1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1] \\
&\quad + [0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1] \\
&= [1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0]
\end{aligned}$$

Chipertext yang diperoleh dari pesan KAMU adalah

100100110111110101011010100100110111011100111110100100110111

111110001101111000000000111000000000.

4.3 Proses Dekripsi

Pada proses dekripsi ini melibatkan penggunaan kunci privat untuk memulihkan pesan asli dari *ciphertext* yang dienkripsi menggunakan kunci publik. Proses ini dimulai dengan menerima *ciphertext* yang telah dienkripsi dengan menggunakan kunci publik G' . Kemudian mengalikan dengan invers dari matriks permutasi P untuk menghapus permutasi yang telah diterapkan pada proses enkripsi. Selanjutnya, penerima menggunakan algoritma decoding untuk mengoreksi kesalahan yang mungkin ada dalam *ciphertext*. Setelah itu, penerima mengalikan hasil tersebut dengan invers dari matriks S untuk menghapus transformasi acak yang diberikan oleh matriks S .

4.3.1 Dekripsi Menggunakan Algoritma McEliece dengan Kode Goppa

1. Input
 - a. *Ciphertext* C_i' dengan panjang n -bit.
 - b. Menghitung invers dari matriks permutasi P .
 - c. Menghitung invers dari matriks S .
 - d. Menentukan matriks *parity check* H .
2. Proses
 - a. Mengalikan *ciphertext* C_i' dengan matriks P^{-1} .
 - b. Mencari *syndrome* $s(x)$ dengan rumus sebagai berikut:

$$s(x) \equiv \sum_{i=1}^n \frac{y_i}{x - \alpha_i}$$

- c. Temukan lokasi *error* $B = \{i | \sigma(\alpha_i) = 0\}$.
- d. Mengoreksi bit *error*, sehingga diperoleh $\hat{m} = mS$.
- e. Mengalikan matriks \hat{m} dengan S^{-1} sehingga diperoleh $m = \hat{m}S^{-1}$.
- f. Binary m_i yang didapatkan dikembalikan kedalam bentuk teks berdasarkan tabel ASCII.

3. Output

Menghasilkan teks sesuai dengan pesan awal.

4.3.2 Simulasi Proses Dekripsi Menggunakan Algoritma McEliece

Proses dekripsi dan pengoreksian error dapat dilakukan setelah penerima pesan menerima ciphertext. Selanjutnya penerima menghitung nilai P^{-1} .

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

Setelah nilai P^{-1} diperoleh, maka kalikan C'_i dikalikan dengan P^{-1} untuk menghasilkan matriks Y_i .

$$\begin{aligned}
Y_7 &= C'_7 \times P^{-1} \\
&= [1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0] \\
&\quad \times \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \\
&= [0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1]
\end{aligned}$$

$$\begin{aligned}
Y_8 &= C'_8 \times P^{-1} \\
&= [1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0] \\
&\quad \times \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \\
&= [0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1]
\end{aligned}$$

Selanjutnya yaitu tahap untuk pengkoreksian *error* dengan mencari nilai dari *syndrome* $s(x)$. Untuk mencari nilai *syndrome* $s(x)$, hitung matriks *parity check* untuk $\Gamma(L, g^2(x))$, dengan $\hat{g}(x) = g^2(t) = (x^2 + \alpha^7 x + 1)^2 = x^4 + \alpha^{14} x^2 + 1$ sebagai polinomial goppa, jadi $\hat{g}_4 = 1, \hat{g}_3 = 0, \hat{g}_2 = \alpha^{14}, \hat{g}_1 = 0$, dan $\hat{g}_0 = 1$. Dimana Faktor \hat{h}_i dihitung dengan

$$\hat{h}_i = (g^2(\alpha_i))^{-1} = (g(\alpha_i)^{-1})^2 = h_i^2.$$

Jadi matriks *parity check* \hat{H} adalah

$$\hat{H} = \begin{pmatrix} ((\alpha^2)^3 + \alpha^{14}\alpha^2)h_1^2 & \dots & ((\alpha^{13})^3 + \alpha^{14}\alpha^{13})h_{12}^2 \\ ((\alpha^2)^2 + \alpha^{14})h_1^2 & \dots & ((\alpha^{13})^2 + \alpha^{14})h_{12}^2 \\ \alpha^2 h_1^2 & \dots & \alpha^{13} h_{12}^2 \\ h_1^2 & \dots & h_{12}^2 \end{pmatrix}$$

$$\hat{H} = \begin{pmatrix} \alpha^5 & \alpha^8 & \alpha^7 & \alpha^3 & \alpha^3 & 0 & \alpha^{13} & \alpha^{10} & \alpha^{14} & \alpha^{10} & \alpha^{10} & \alpha^{10} \\ \alpha^3 & \alpha^5 & \alpha^3 & \alpha^{13} & \alpha^{12} & 0 & \alpha^5 & 1 & \alpha^4 & \alpha^{14} & \alpha^{13} & \alpha^{12} \\ \alpha^{11} & 1 & \alpha & \alpha^7 & \alpha^{13} & \alpha^7 & \alpha^6 & \alpha^{10} & \alpha^2 & \alpha^9 & \alpha^6 & 1 \\ \alpha^9 & \alpha^{12} & \alpha^{12} & \alpha^2 & \alpha^7 & 1 & \alpha^{13} & \alpha & \alpha^7 & \alpha^{13} & \alpha^9 & \alpha^2 \end{pmatrix}$$

Setelah matriks *parity check* H didapatkan, selanjutnya mencari *syndrome*

$s(x)$ sebagai berikut :

a. Cari sindrom $s(x)$ dari

$$Y_1 = C_1' \times P^{-1} = [1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1]$$

$$\begin{aligned} s(x) &= \sum_{i=1}^{12} \frac{y_i}{x - \alpha_i} \\ &= \frac{1}{x - \alpha^2} + \frac{1}{x - \alpha^3} + \frac{1}{x - \alpha^7} + \frac{1}{x - \alpha^8} + \frac{1}{x - \alpha^{10}} + \frac{1}{x - \alpha^{11}} \\ &\quad + \frac{1}{x - \alpha^{13}} \\ &= (\alpha^5 + \alpha^8 + 0 + \alpha^{13} + \alpha^{14} + \alpha^{10} + \alpha^{10}) + (\alpha^3 + \alpha^5 + 0 + \alpha^5 \\ &\quad + \alpha^4 + \alpha^{14} + \alpha^{12})x + (\alpha^{11} + 1 + \alpha^7 + \alpha^6 + \alpha^2 \\ &\quad + \alpha^9 + 1)x^2 + (\alpha^9 + \alpha^{12} + 1 + \alpha^{13} + \alpha^7 + \alpha^{13} \\ &\quad + \alpha^2)x^3 \end{aligned}$$

$$\begin{aligned}
&= (\alpha + \alpha^2 + 1 + \alpha^2 + 0 + 1 + \alpha^2 + \alpha^3 + 1 + \alpha^3 + 1 + \alpha + \alpha^2 \\
&\quad + 1 + \alpha + \alpha^2) + (\alpha^3 + \alpha + \alpha^2 + 0 + \alpha + \alpha^2 + 1 \\
&\quad + \alpha + 1 + \alpha^3 + 1 + \alpha + \alpha^2 + \alpha^3)x \\
&\quad + (\alpha + \alpha^2 + \alpha^3 + 1 + 1 + \alpha + \alpha^3 + \alpha^2 + \alpha^3 + \alpha^2 \\
&\quad + \alpha + \alpha^3 + 1)x^2 \\
&\quad + (\alpha + \alpha^3 + 1 + \alpha + \alpha^2 + \alpha^3 + 1 + 1 + \alpha^2 + \alpha^3 \\
&\quad + 1 + \alpha + \alpha^3 + 1 + \alpha^2 + \alpha^3 + \alpha^2)x^3 \\
&= (1 + \alpha + \alpha^2) + (1 + \alpha^2 + \alpha^3)x + (1 + \alpha + \alpha^2)x^2 \\
&\quad + (1 + \alpha + \alpha^3)x^3 \\
&= \alpha^7 x^3 + \alpha^{10} x^2 + \alpha^{13} x + \alpha^{10}
\end{aligned}$$

Selesaikan $\sigma(x)s(x) \pmod{(x^4 + \alpha^{14}x^2 + 1)}$,

$$\begin{aligned}
\sigma(x)s(x) &= (x^2 + \sigma_1 x + \sigma_0)(\alpha^7 x^3 + \alpha^{10} x^2 + \alpha^{13} x + \alpha^{10}) \\
&= \alpha^7 x^5 + (\alpha^7 \sigma_1 + \alpha^{10})x^4 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{13})x^3 \\
&\quad + (\alpha^{13} \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10})x^2 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^{13} \sigma_0)x + \alpha^{10} \sigma_0
\end{aligned}$$

$$\begin{aligned}
\sigma(x)s(x) \pmod{(x' = (\alpha^{14}x^3 + x) + (\alpha^7 \sigma_1 + \alpha^{10})(\alpha^{14}x^2 + 1) \\
+ \alpha^{14}x^2 + 1)) &= (\alpha^{14}x^3 + x) + (\alpha^7 \sigma_1 + \alpha^{10})(\alpha^{14}x^2 + 1) \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{13})x^3 \\
&\quad + (\alpha^{13} \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10})x^2 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^{13} \sigma_0)x + \alpha^{10} \sigma_0
\end{aligned}$$

$$\begin{aligned}
&= (\alpha^{10}\sigma_1 + \alpha^7\sigma_0 + \alpha^{13} + \alpha^6)x^3 \\
&\quad + (\alpha^{13}\sigma_1 + \alpha^6\sigma_1 + \alpha^{10}\sigma_0 + \alpha^{10} \\
&\quad + \alpha^9)x^2 + (\alpha^{10}\sigma_1 + \alpha^{13}\sigma_0 + \alpha^7)x \\
&\quad + (\alpha^7\sigma_1 + \alpha^{10}\sigma_0 + \alpha^{10})
\end{aligned}$$

Kemudian substitusikan persamaan di atas ke

$$\sigma(x)s(x) \equiv \sigma'(x) \pmod{(x^4 + \alpha^{14}x^2 + 1)}$$

Oleh karena itu, perlu menyelesaikan sistem persamaan berikut untuk mendapatkan nilai dari σ_1 dan σ_0 .

$$\begin{cases}
\alpha^{10}\sigma_1 + \alpha^7\sigma_0 + \alpha^{13} + \alpha^6 = 0 \\
\alpha^{10}\sigma_1 + \alpha^{13}\sigma_0 + \alpha^7 = 0
\end{cases}$$

Didapatkan $\sigma_0 = \alpha^4$ dan $\sigma_1 = \alpha^2$, sehingga

$$\sigma(x) = x^2 + \alpha^2x + \alpha^4 = (x + \alpha^7)(x + \alpha^{12})$$

Karena $\alpha_6 = \alpha^7$ dan $\alpha_{11} = \alpha^{12}$, maka diperoleh himpunan lokasi *error*-nya adalah

$$B = \{i \mid \sigma(\alpha_i) = 0\} = \{6, 11\}$$

Sehingga dapat di temukan vektor *error* $e' = [0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0]$, kemudian

$$Y'_1 = Y_1 - e' = [1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1]$$

Setelah Y_1 dikoreksi didapatkan Y'_1 dan karena Y'_1 dihasilkan dari *standard form generator matriks* yang mana 4 bit dari kiri merupakan pesan informasi atau data bit, dan 8 bit dari kanan merupakan *parity* bit. Maka dapat diambil 4 bit *binary* Y'_1 dari kiri.

$$\hat{m}_1 = [1 \ 1 \ 0 \ 0]$$

b. Cari sindrom $s(x)$ dari

$$Y_2 = C'_2 \times P^{-1} = [1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1]$$

$$\begin{aligned} s(x) &= \sum_{i=1}^{12} \frac{y_i}{x - \alpha_i} \\ &= \frac{1}{x - \alpha^2} + \frac{1}{x - \alpha^6} + \frac{1}{x - \alpha^9} + \frac{1}{x - \alpha^{10}} + \frac{1}{x - \alpha^{11}} + \frac{1}{x - \alpha^{12}} \\ &\quad + \frac{1}{x - \alpha^{13}} \\ &= (\alpha^5 + \alpha^3 + \alpha^{10} + \alpha^{14} + \alpha^{10} + \alpha^{10} + \alpha^{10}) + (\alpha^3 + \alpha^{12} + 1 + \alpha^4 \\ &\quad + \alpha^{14} + \alpha^{13} + \alpha^{12})x + (\alpha^{11} + \alpha^{13} + \alpha^{10} + \alpha^2 + \alpha^9 \\ &\quad + \alpha^6 + 1)x^2 + (\alpha^9 + \alpha^7 + \alpha + \alpha^7 + \alpha^{13} + \alpha^9 \\ &\quad + \alpha^2)x^3 \\ &= (\alpha + \alpha^2 + \alpha^3 + 1 + \alpha + \alpha^2 + 1 + \alpha^3 + 1 + \alpha + \alpha^2 + 1 + \alpha \\ &\quad + \alpha^2 + 1 + \alpha + \alpha^2) + (\alpha^3 + 1 + \alpha + \alpha^2 + \alpha^3 + 1 \\ &\quad + 1 + \alpha + 1 + \alpha^3 + 1 + \alpha^2 + \alpha^3 + 1 + \alpha + \alpha^2 \\ &\quad + \alpha^3)x \\ &\quad + (\alpha + \alpha^2 + \alpha^3 + 1 + \alpha^2 + \alpha^3 + 1 + \alpha + \alpha^2 + \alpha^2 \\ &\quad + \alpha + \alpha^3 + \alpha^2 + \alpha^3 + 1)x^2 \\ &\quad + (\alpha + \alpha^3 + 1 + \alpha + \alpha^3 + \alpha + 1 + \alpha + \alpha^3 + 1 + \alpha^2 \\ &\quad + \alpha^3 + \alpha + \alpha^3 + \alpha^2)x^3 \\ &= (1 + \alpha + \alpha^2) + (\alpha + \alpha^2 + \alpha^3)x + (1 + \alpha + \alpha^2)x^2 \\ &\quad + (1 + \alpha + \alpha^3)x^3 \\ &= \alpha^7 x^3 + \alpha^{10} x^2 + \alpha^{11} x + \alpha^{10} \end{aligned}$$

Selesaikan $\sigma(x)s(x) \pmod{(x^4 + \alpha^{14}x^2 + 1)}$,

$$\begin{aligned}
\sigma(x)s(x) &= (x^2 + \sigma_1 x + \sigma_0)(\alpha^7 x^3 + \alpha^{10} x^2 + \alpha^{11} x + \alpha^{10}) \\
&= \alpha^7 x^5 + (\alpha^7 \sigma_1 + \alpha^{10})x^4 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{11})x^3 \\
&\quad + (\alpha^{11} \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10})x^2 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^{11} \sigma_0)x + \alpha^{10} \sigma_0 \\
&= \alpha^7(\alpha^{14} x^3 + x) + (\alpha^7 \sigma_1 + \alpha^{10})(\alpha^{14} x^2 + 1) \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{11})x^3 \\
&\quad + (\alpha^{11} \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10})x^2 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^{11} \sigma_0)x + \alpha^{10} \sigma_0 \\
\sigma(x)s(x)(\text{mod } (x^4 &= (\alpha^6 x^3 + \alpha^7 x) + (\alpha^6 \sigma_1 x^2 + \alpha^7 \sigma_1 + \alpha^9 x^2 + \alpha^{10}) \\
+ \alpha^{14} x^2 + 1)) &\quad + (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{11})x^3 \\
&\quad + (\alpha^{11} \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10})x^2 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^{11} \sigma_0)x + \alpha^{10} \sigma_0 \\
&= (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{11} + \alpha^6)x^3 \\
&\quad + (\alpha^{11} \sigma_1 + \alpha^6 \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10} \\
&\quad + \alpha^9)x^2 + (\alpha^{10} \sigma_1 + \alpha^{11} \sigma_0 + \alpha^7)x \\
&\quad + (\alpha^7 \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10})
\end{aligned}$$

Kemudian substitusikan persamaan di atas ke

$$\sigma(x)s(x) \equiv \sigma'(x) \pmod{(x^4 + \alpha^{14} x^2 + 1)}$$

Oleh karena itu, perlu menyelesaikan sistem persamaan berikut untuk mendapatkan nilai dari σ_1 dan σ_0 .

$$\begin{cases} \alpha^{10} \sigma_1 + \alpha^{11} \sigma_0 + \alpha^7 = 0 \\ \alpha^7 \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10} = 0 \end{cases}$$

Didapatkan $\sigma_0 = \alpha$ dan $\sigma_1 = \alpha^7$, sehingga

$$\sigma(x) = x^2 + \alpha^7 x + \alpha = (x + \alpha^6)(x + \alpha^{10})$$

Karena $\alpha_5 = \alpha^6$ dan $\alpha_9 = \alpha^{10}$, maka diperoleh himpunan lokasi *error*nya adalah

$$B = \{i \mid \sigma(\alpha_i) = 0\} = \{5, 9\}$$

Sehingga dapat ditemukan vektor *error* $e' = [0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0]$, kemudian

$$Y'_2 = Y_2 - e' = [1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1]$$

Setelah Y_2 dikoreksi didapatkan Y'_2 dan karena Y'_2 dihasilkan dari *standard form generator matriks* yang mana 4 bit dari kiri merupakan pesan informasi atau data bit, dan 8 bit dari kanan merupakan *parity* bit. Maka dapat diambil 4 bit *binary* Y'_2 dari kiri.

$$\hat{m}_2 = [1 \ 0 \ 0 \ 0]$$

c. Cari sindrom $s(x)$ dari

$$Y_3 = C'_3 \times P^{-1} = [1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 1]$$

$$\begin{aligned} s(x) &= \sum_{i=1}^{12} \frac{y_i}{x - \alpha_i} \\ &= \frac{1}{x - \alpha^2} + \frac{1}{x - \alpha^3} + \frac{1}{x - \alpha^7} + \frac{1}{x - \alpha^8} + \frac{1}{x - \alpha^{10}} + \frac{1}{x - \alpha^{11}} \\ &\quad + \frac{1}{x - \alpha^{13}} \\ &= (\alpha^5 + \alpha^8 + 0 + \alpha^{13} + \alpha^{14} + \alpha^{10} + \alpha^{10}) + (\alpha^3 + \alpha^5 + 0 + \alpha^5 \\ &\quad + \alpha^4 + \alpha^{14} + \alpha^{12})x + (\alpha^{11} + 1 + \alpha^7 + \alpha^6 + \alpha^2 \\ &\quad + \alpha^9 + 1)x^2 + (\alpha^9 + \alpha^{12} + 1 + \alpha^{13} + \alpha^7 + \alpha^{13} \\ &\quad + \alpha^2)x^3 \end{aligned}$$

$$\begin{aligned}
&= (\alpha + \alpha^2 + 1 + \alpha^2 + 0 + 1 + \alpha^2 + \alpha^3 + 1 + \alpha^3 + 1 + \alpha + \alpha^2 \\
&\quad + 1 + \alpha + \alpha^2) + (\alpha^3 + \alpha + \alpha^2 + 0 + \alpha + \alpha^2 + 1 \\
&\quad + \alpha + 1 + \alpha^3 + 1 + \alpha + \alpha^2 + \alpha^3)x \\
&\quad + (\alpha + \alpha^2 + \alpha^3 + 1 + 1 + \alpha + \alpha^3 + \alpha^2 + \alpha^3 + \alpha^2 \\
&\quad + \alpha + \alpha^3 + 1)x^2 \\
&\quad + (\alpha + \alpha^3 + 1 + \alpha + \alpha^2 + \alpha^3 + 1 + 1 + \alpha^2 + \alpha^3 \\
&\quad + 1 + \alpha + \alpha^3 + 1 + \alpha^2 + \alpha^3 + \alpha^2)x^3 \\
&= (1 + \alpha + \alpha^2) + (1 + \alpha^2 + \alpha^3)x + (1 + \alpha + \alpha^2)x^2 \\
&\quad + (1 + \alpha + \alpha^3)x^3 \\
&= \alpha^7 x^3 + \alpha^{10} x^2 + \alpha^{13} x + \alpha^{10}
\end{aligned}$$

Selesaikan $\sigma(x)s(x) \pmod{(x^4 + \alpha^{14}x^2 + 1)}$,

$$\begin{aligned}
\sigma(x)s(x) &= (x^2 + \sigma_1 x + \sigma_0)(\alpha^7 x^3 + \alpha^{10} x^2 + \alpha^{13} x + \alpha^{10}) \\
&= \alpha^7 x^5 + (\alpha^7 \sigma_1 + \alpha^{10})x^4 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{13})x^3 \\
&\quad + (\alpha^{13} \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10})x^2 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^{13} \sigma_0)x + \alpha^{10} \sigma_0 \\
\sigma(x)s(x) \pmod{(x^4 + \alpha^{14}x^2 + 1)} &= \alpha^7 (\alpha^{14} x^3 + x) + (\alpha^7 \sigma_1 + \alpha^{10})(\alpha^{14} x^2 + 1) \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{13})x^3 \\
&\quad + (\alpha^{13} \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10})x^2 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^{13} \sigma_0)x + \alpha^{10} \sigma_0
\end{aligned}$$

$$\begin{aligned}
&= (\alpha^6 x^3 + \alpha^7 x) + (\alpha^6 \sigma_1 x^2 + \alpha^7 \sigma_1 + \alpha^9 x^2 + \alpha^{10}) \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{13}) x^3 \\
&\quad + (\alpha^{13} \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10}) x^2 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^{13} \sigma_0) x + \alpha^{10} \sigma_0 \\
&= (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{13} + \alpha^6) x^3 \\
&\quad + (\alpha^{13} \sigma_1 + \alpha^6 \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10} \\
&\quad + \alpha^9) x^2 + (\alpha^{10} \sigma_1 + \alpha^{13} \sigma_0 + \alpha^7) x \\
&\quad + (\alpha^7 \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10})
\end{aligned}$$

Kemudian substitusikan persamaan di atas ke

$$\sigma(x)s(x) \equiv \sigma'(x) \pmod{(x^4 + \alpha^{14}x^2 + 1)}$$

Oleh karena itu, perlu menyelesaikan sistem persamaan berikut untuk mendapatkan nilai dari σ_1 dan σ_0 .

$$\begin{cases} \alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{13} + \alpha^6 = 0 \\ \alpha^{10} \sigma_1 + \alpha^{13} \sigma_0 + \alpha^7 = 0 \end{cases}$$

Didapatkan $\sigma_0 = \alpha^4$ dan $\sigma_1 = \alpha^2$, sehingga

$$\sigma(x) = x^2 + \alpha^2 x + \alpha^4 = (x + \alpha^7)(x + \alpha^{12})$$

Karena $\alpha_6 = \alpha^7$ dan $\alpha_{11} = \alpha^{12}$, maka diperoleh himpunan lokasi *error*nya adalah

$$B = \{i \mid \sigma(\alpha_i) = 0\} = \{6, 11\}$$

Sehingga dapat ditemukan vektor *error* $e' =$

$[0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0]$, kemudian

$$Y'_3 = Y_3 - e' = [1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1]$$

Setelah Y_3 dikoreksi didapatkan Y'_3 dan karena Y'_3 dihasilkan dari *standard form generator matriks* yang mana 4 bit dari kiri merupakan pesan informasi atau data

bit, dan 8 bit dari kanan merupakan *parity* bit. Maka dapat diambil 4 bit *binary* Y'_3 dari kiri.

$$\hat{m}_3 = [1 \ 1 \ 0 \ 0]$$

d. Cari sindrom $s(x)$ dari

$$Y_4 = C'_4 \times P^{-1} = [1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0]$$

$$\begin{aligned} s(x) &= \sum_{i=1}^{12} \frac{y_i}{x - \alpha_i} \\ &= \frac{1}{x - \alpha^2} + \frac{1}{x - \alpha^3} + \frac{1}{x - \alpha^5} + \frac{1}{x - \alpha^6} + \frac{1}{x - \alpha^8} + \frac{1}{x - \alpha^{10}} \\ &\quad + \frac{1}{x - \alpha^{11}} + \frac{1}{x - \alpha^{12}} \\ &= (\alpha^5 + \alpha^8 + \alpha^3 + \alpha^3 + \alpha^{13} + \alpha^{14} + \alpha^{10} + \alpha^{10}) + (\alpha^3 + \alpha^5 \\ &\quad + \alpha^{13} + \alpha^{12} + \alpha^5 + \alpha^4 + \alpha^{14} + \alpha^{13})x + (\alpha^{11} + 1 \\ &\quad + \alpha^7 + \alpha^{13} + \alpha^6 + \alpha^2 + \alpha^9 + \alpha^6)x^2 + (\alpha^9 + \alpha^{12} \\ &\quad + \alpha^2 + \alpha^7 + \alpha^{13} + \alpha^7 + \alpha^{13} + \alpha^9)x^3 \\ &= (\alpha + \alpha^2 + 1 + \alpha^2 + \alpha^3 + 1 + \alpha^2 + \alpha^3 + 1 + \alpha^3 + 1 + \alpha + \alpha^2 \\ &\quad + 1 + \alpha + \alpha^2) + (\alpha^3 + \alpha + \alpha^2 + 1 + \alpha^2 + \alpha^3 \\ &\quad + 1 + \alpha + \alpha^2 + \alpha^3 + \alpha + \alpha^2 + 1 + \alpha + 1 + \alpha^3 \\ &\quad + 1 + \alpha^2 + \alpha^3)x \\ &\quad + (\alpha + \alpha^2 + \alpha^3 + 1 + 1 + \alpha + \alpha^3 + 1 + \alpha^2 + \alpha^3 \\ &\quad + \alpha^2 + \alpha^3 + \alpha^2 + \alpha + \alpha^3 + \alpha^2 + \alpha^3)x^2 \\ &\quad + (\alpha + \alpha^3 + 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^2 + 1 + \alpha + \alpha^3 \\ &\quad + 1 + \alpha^2 + \alpha^3 + 1 + \alpha + \alpha^3 + 1 + \alpha^2 + \alpha^3 \\ &\quad + \alpha + \alpha^3)x^3 \end{aligned}$$

$$\begin{aligned}
&= (1 + \alpha + \alpha^2) + (1 + \alpha^2 + \alpha^3)x + (1 + \alpha + \alpha^2)x^2 \\
&\quad + (1 + \alpha + \alpha^3)x^3 \\
&= \alpha^7 x^3 + \alpha^{10} x^2 + \alpha^{13} x + \alpha^{10}
\end{aligned}$$

Selesaikan $\sigma(x)s(x) \pmod{(x^4 + \alpha^{14}x^2 + 1)}$,

$$\begin{aligned}
\sigma(x)s(x) &= (x^2 + \sigma_1 x + \sigma_0)(\alpha^7 x^3 + \alpha^{10} x^2 + \alpha^{13} x + \alpha^{10}) \\
&= \alpha^7 x^5 + (\alpha^7 \sigma_1 + \alpha^{10})x^4 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{13})x^3 \\
&\quad + (\alpha^{13} \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10})x^2 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^{13} \sigma_0)x + \alpha^{10} \sigma_0
\end{aligned}$$

$$\begin{aligned}
\sigma(x)s(x) \pmod{(x^4 + \alpha^{14}x^2 + 1)} &= \alpha^7(\alpha^{14}x^3 + x) + (\alpha^7 \sigma_1 + \alpha^{10})(\alpha^{14}x^2 + 1) \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{13})x^3 \\
&\quad + (\alpha^{13} \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10})x^2 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^{13} \sigma_0)x + \alpha^{10} \sigma_0 \\
&= (\alpha^6 x^3 + \alpha^7 x) + (\alpha^6 \sigma_1 x^2 + \alpha^7 \sigma_1 + \alpha^9 x^2 + \alpha^{10}) \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{13})x^3 \\
&\quad + (\alpha^{13} \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10})x^2 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^{13} \sigma_0)x + \alpha^{10} \sigma_0 \\
&= (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{13} + \alpha^6)x^3 \\
&\quad + (\alpha^{13} \sigma_1 + \alpha^6 \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10} \\
&\quad + \alpha^9)x^2 + (\alpha^{10} \sigma_1 + \alpha^{13} \sigma_0 + \alpha^7)x \\
&\quad + (\alpha^7 \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10})
\end{aligned}$$

Kemudian substitusikan persamaan di atas ke

$$\sigma(x)s(x) \equiv \sigma'(x) \pmod{(x^4 + \alpha^{14}x^2 + 1)}$$

Oleh karena itu, perlu menyelesaikan sistem persamaan berikut untuk mendapatkan nilai dari σ_1 dan σ_0 .

$$\begin{cases} \alpha^{10}\sigma_1 + \alpha^7\sigma_0 + \alpha^{13} + \alpha^6 = 0 \\ \alpha^{10}\sigma_1 + \alpha^{13}\sigma_0 + \alpha^7 = 0 \end{cases}$$

Didapatkan $\sigma_0 = \alpha^4$ dan $\sigma_1 = \alpha^2$, sehingga

$$\sigma(x) = x^2 + \alpha^2x + \alpha^4 = (x + \alpha^7)(x + \alpha^{12})$$

Karena $\alpha_6 = \alpha^7$ dan $\alpha_{11} = \alpha^{12}$, maka diperoleh himpunan lokasi *error*nya adalah

$$B = \{i \mid \sigma(\alpha_i) = 0\} = \{6, 11\}$$

Sehingga dapat ditemukan vektor *error* $e' = [0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0]$, kemudian

$$Y'_4 = Y_4 - e' = [1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0]$$

Setelah Y_4 dikoreksi didapatkan Y'_4 dan karena Y'_4 dihasilkan dari *standard form generator matriks* yang mana 4 bit dari kiri merupakan pesan informasi atau data bit, dan 8 bit dari kanan merupakan *parity* bit. Maka dapat diambil 4 bit *binary* Y'_4 dari kiri.

$$\hat{m}_4 = [1 \ 1 \ 0 \ 1]$$

e. Cari sindrom $s(x)$ dari

$$Y_5 = C'_5 \times P^{-1} = [1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 1]$$

$$\begin{aligned} s(x) &= \sum_{i=1}^{12} \frac{y_i}{x - \alpha_i} \\ &= \frac{1}{x - \alpha^2} + \frac{1}{x - \alpha^3} + \frac{1}{x - \alpha^7} + \frac{1}{x - \alpha^8} + \frac{1}{x - \alpha^{10}} + \frac{1}{x - \alpha^{11}} \\ &\quad + \frac{1}{x - \alpha^{13}} \end{aligned}$$

$$\begin{aligned}
&= (\alpha^5 + \alpha^8 + 0 + \alpha^{13} + \alpha^{14} + \alpha^{10} + \alpha^{10}) + (\alpha^3 + \alpha^5 + 0 + \alpha^5 \\
&\quad + \alpha^4 + \alpha^{14} + \alpha^{12})x + (\alpha^{11} + 1 + \alpha^7 + \alpha^6 + \alpha^2 \\
&\quad + \alpha^9 + 1)x^2 + (\alpha^9 + \alpha^{12} + 1 + \alpha^{13} + \alpha^7 + \alpha^{13} \\
&\quad + \alpha^2)x^3 \\
&= (\alpha + \alpha^2 + 1 + \alpha^2 + 0 + 1 + \alpha^2 + \alpha^3 + 1 + \alpha^3 + 1 + \alpha + \alpha^2 \\
&\quad + 1 + \alpha + \alpha^2) + (\alpha^3 + \alpha + \alpha^2 + 0 + \alpha + \alpha^2 + 1 \\
&\quad + \alpha + 1 + \alpha^3 + 1 + \alpha + \alpha^2 + \alpha^3)x \\
&\quad + (\alpha + \alpha^2 + \alpha^3 + 1 + 1 + \alpha + \alpha^3 + \alpha^2 + \alpha^3 + \alpha^2 \\
&\quad + \alpha + \alpha^3 + 1)x^2 \\
&\quad + (\alpha + \alpha^3 + 1 + \alpha + \alpha^2 + \alpha^3 + 1 + 1 + \alpha^2 + \alpha^3 \\
&\quad + 1 + \alpha + \alpha^3 + 1 + \alpha^2 + \alpha^3 + \alpha^2)x^3 \\
&= (1 + \alpha + \alpha^2) + (1 + \alpha^2 + \alpha^3)x + (1 + \alpha + \alpha^2)x^2 \\
&\quad + (1 + \alpha + \alpha^3)x^3 \\
&= \alpha^7 x^3 + \alpha^{10} x^2 + \alpha^{13} x + \alpha^{10}
\end{aligned}$$

Selesaikan $\sigma(x)s(x) \pmod{(x^4 + \alpha^{14}x^2 + 1)}$,

$$\begin{aligned}
\sigma(x)s(x) &= (x^2 + \sigma_1 x + \sigma_0)(\alpha^7 x^3 + \alpha^{10} x^2 + \alpha^{13} x + \alpha^{10}) \\
&= \alpha^7 x^5 + (\alpha^7 \sigma_1 + \alpha^{10})x^4 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{13})x^3 \\
&\quad + (\alpha^{13} \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10})x^2 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^{13} \sigma_0)x + \alpha^{10} \sigma_0
\end{aligned}$$

$$\begin{aligned}
\sigma(x)s(x) \pmod{(x^4 + \alpha^7(\alpha^{14}x^3 + x) + (\alpha^7\sigma_1 + \alpha^{10})(\alpha^{14}x^2 + 1) + \alpha^{14}x^2 + 1)} &= \alpha^7(\alpha^{14}x^3 + x) + (\alpha^7\sigma_1 + \alpha^{10})(\alpha^{14}x^2 + 1) \\
&+ (\alpha^{10}\sigma_1 + \alpha^7\sigma_0 + \alpha^{13})x^3 \\
&+ (\alpha^{13}\sigma_1 + \alpha^{10}\sigma_0 + \alpha^{10})x^2 \\
&+ (\alpha^{10}\sigma_1 + \alpha^{13}\sigma_0)x + \alpha^{10}\sigma_0 \\
&= (\alpha^6x^3 + \alpha^7x) + (\alpha^6\sigma_1x^2 + \alpha^7\sigma_1 + \alpha^9x^2 + \alpha^{10}) \\
&+ (\alpha^{10}\sigma_1 + \alpha^7\sigma_0 + \alpha^{13})x^3 \\
&+ (\alpha^{13}\sigma_1 + \alpha^{10}\sigma_0 + \alpha^{10})x^2 \\
&+ (\alpha^{10}\sigma_1 + \alpha^{13}\sigma_0)x + \alpha^{10}\sigma_0 \\
&= (\alpha^{10}\sigma_1 + \alpha^7\sigma_0 + \alpha^{13} + \alpha^6)x^3 \\
&+ (\alpha^{13}\sigma_1 + \alpha^6\sigma_1 + \alpha^{10}\sigma_0 + \alpha^{10} \\
&+ \alpha^9)x^2 + (\alpha^{10}\sigma_1 + \alpha^{13}\sigma_0 + \alpha^7)x \\
&+ (\alpha^7\sigma_1 + \alpha^{10}\sigma_0 + \alpha^{10})
\end{aligned}$$

Kemudian substitusikan persamaan di atas ke

$$\sigma(x)s(x) \equiv \sigma'(x) \pmod{x^4 + \alpha^{14}x^2 + 1}$$

Oleh karena itu, perlu menyelesaikan sistem persamaan berikut untuk mendapatkan nilai dari σ_1 dan σ_0 .

$$\begin{cases} \alpha^{10}\sigma_1 + \alpha^7\sigma_0 + \alpha^{13} + \alpha^6 = 0 \\ \alpha^{10}\sigma_1 + \alpha^{13}\sigma_0 + \alpha^7 = 0 \end{cases}$$

Didapatkan $\sigma_0 = \alpha^4$ dan $\sigma_1 = \alpha^2$, sehingga

$$\sigma(x) = x^2 + \alpha^2x + \alpha^4 = (x + \alpha^7)(x + \alpha^{12})$$

Karena $\alpha_6 = \alpha^7$ dan $\alpha_{11} = \alpha^{12}$, maka diperoleh himpunan lokasi *error*-nya adalah

$$B = \{i \mid \sigma(\alpha_i) = 0\} = \{6, 11\}$$

Sehingga dapat ditemukan vektor *error* $e' = [0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0]$, kemudian

$$Y'_5 = Y_5 - e' = [1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1]$$

Setelah Y_5 dikoreksi didapatkan Y'_5 dan karena Y'_5 dihasilkan dari *standard form generator matriks* yang mana 4 bit dari kiri merupakan pesan informasi atau data bit, dan 8 bit dari kanan merupakan *parity* bit. Maka dapat diambil 4 bit *binary* Y'_5 dari kiri.

$$\hat{m}_5 = [1 \ 1 \ 0 \ 0]$$

f. Cari sindrom $s(x)$ dari

$$Y_6 = C'_6 \times P^{-1} = [0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1]$$

$$\begin{aligned} s(x) &= \sum_{i=1}^{12} \frac{y_i}{x - \alpha_i} \\ &= \frac{1}{x - \alpha^3} + \frac{1}{x - \alpha^4} + \frac{1}{x - \alpha^5} + \frac{1}{x - \alpha^6} + \frac{1}{x - \alpha^7} + \frac{1}{x - \alpha^{10}} \\ &\quad + \frac{1}{x - \alpha^{12}} + \frac{1}{x - \alpha^{13}} \\ &= (\alpha^8 + \alpha^7 + \alpha^3 + \alpha^3 + 0 + \alpha^{14} + \alpha^{10} + \alpha^{10}) + (\alpha^5 + \alpha^3 + \alpha^{13} \\ &\quad + \alpha^{12} + 0 + \alpha^4 + \alpha^{13} + \alpha^{12})x + (1 + \alpha + \alpha^7 + \alpha^{13} \\ &\quad + \alpha^7 + \alpha^2 + \alpha^6 + 1)x^2 + (\alpha^{12} + \alpha^{12} + \alpha^2 + \alpha^7 + 1 \\ &\quad + \alpha^7 + \alpha^9 + \alpha^2)x^3 \end{aligned}$$

$$\begin{aligned}
&= (1 + \alpha^2 + 1 + \alpha + \alpha^3 + \alpha^3 + \alpha^3 + 0 + 1 + \alpha^3 + 1 + \alpha + \alpha^2 \\
&\quad + 1 + \alpha + \alpha^2) + (\alpha + \alpha^2 + \alpha^3 + 1 + \alpha^2 + \alpha^3 \\
&\quad + 1 + \alpha + \alpha^2 + \alpha^3 + 0 + 1 + \alpha + 1 + \alpha^2 + \alpha^3 \\
&\quad + 1 + \alpha + \alpha^2 + \alpha^3)x \\
&\quad + (1 + \alpha + 1 + \alpha + \alpha^3 + 1 + \alpha^2 + \alpha^3 + 1 + \alpha + \alpha^3 \\
&\quad + \alpha^2 + \alpha^2 + \alpha^3 + 1)x^2 \\
&\quad + (1 + \alpha + \alpha^2 + \alpha^3 + 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^2 \\
&\quad + 1 + \alpha + \alpha^3 + 1 + 1 + \alpha + \alpha^3 + \alpha + \alpha^3 + \alpha^2)x^3 \\
&= (1 + \alpha + \alpha^2) + (1 + \alpha^2 + \alpha^3)x + (1 + \alpha + \alpha^2)x^2 \\
&\quad + (1 + \alpha + \alpha^3)x^3 \\
&= \alpha^7 x^3 + \alpha^{10} x^2 + \alpha^{13} x + \alpha^{10}
\end{aligned}$$

Selesaikan $\sigma(x)s(x) \pmod{(x^4 + \alpha^{14}x^2 + 1)}$,

$$\begin{aligned}
\sigma(x)s(x) &= (x^2 + \sigma_1 x + \sigma_0)(\alpha^7 x^3 + \alpha^{10} x^2 + \alpha^{13} x + \alpha^{10}) \\
&= \alpha^7 x^5 + (\alpha^7 \sigma_1 + \alpha^{10})x^4 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{13})x^3 \\
&\quad + (\alpha^{13} \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10})x^2 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^{13} \sigma_0)x + \alpha^{10} \sigma_0 \\
\sigma(x)s(x) \pmod{(x^4 + \alpha^{14}x^2 + 1)} &= \alpha^7(\alpha^{14}x^3 + x) + (\alpha^7 \sigma_1 + \alpha^{10})(\alpha^{14}x^2 + 1) \\
&\quad + \alpha^{14}x^2 + 1) \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{13})x^3 \\
&\quad + (\alpha^{13} \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10})x^2 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^{13} \sigma_0)x + \alpha^{10} \sigma_0
\end{aligned}$$

$$\begin{aligned}
&= (\alpha^6 x^3 + \alpha^7 x) + (\alpha^6 \sigma_1 x^2 + \alpha^7 \sigma_1 + \alpha^9 x^2 + \alpha^{10}) \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{13}) x^3 \\
&\quad + (\alpha^{13} \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10}) x^2 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^{13} \sigma_0) x + \alpha^{10} \sigma_0 \\
&= (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{13} + \alpha^6) x^3 \\
&\quad + (\alpha^{13} \sigma_1 + \alpha^6 \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10} \\
&\quad + \alpha^9) x^2 + (\alpha^{10} \sigma_1 + \alpha^{13} \sigma_0 + \alpha^7) x \\
&\quad + (\alpha^7 \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10})
\end{aligned}$$

Kemudian substitusikan persamaan di atas ke

$$\sigma(x)s(x) \equiv \sigma'(x) \pmod{(x^4 + \alpha^{14}x^2 + 1)}$$

Oleh karena itu, perlu menyelesaikan sistem persamaan berikut untuk mendapatkan nilai dari σ_1 dan σ_0 .

$$\begin{cases} \alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{13} + \alpha^6 = 0 \\ \alpha^{10} \sigma_1 + \alpha^{13} \sigma_0 + \alpha^7 = 0 \end{cases}$$

Didapatkan $\sigma_0 = \alpha^4$ dan $\sigma_1 = \alpha^2$, sehingga

$$\sigma(x) = x^2 + \alpha^2 x + \alpha^4 = (x + \alpha^7)(x + \alpha^{12})$$

Karena $\alpha_6 = \alpha^7$ dan $\alpha_{11} = \alpha^{12}$, maka diperoleh himpunan lokasi *error*nya adalah

$$B = \{i \mid \sigma(\alpha_i) = 0\} = \{6, 11\}$$

Sehingga dapat ditemukan vektor *error* $e' =$

$[0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0]$, kemudian

$$Y'_6 = Y_6 - e' = [0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1]$$

Setelah Y_6 dikoreksi didapatkan Y'_6 dan karena Y'_6 dihasilkan dari *standard form generator matriks* yang mana 4 bit dari kiri merupakan pesan informasi atau data bit, dan 8 bit dari kanan merupakan *parity* bit. Maka dapat diambil 4 bit *binary* Y'_6 dari kiri.

$$\hat{m}_6 = [0 \quad 1 \quad 1 \quad 1]$$

g. Cari sindrom $s(x)$ dari

$$Y_7 = C'_7 \times P^{-1} = [0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1]$$

$$\begin{aligned} s(x) &= \sum_{i=1}^{12} \frac{y_i}{x - \alpha_i} \\ &= \frac{1}{x - \alpha^5} + \frac{1}{x - \alpha^6} + \frac{1}{x - \alpha^{13}} \\ &= (\alpha^3 + \alpha^3 + \alpha^{10}) + (\alpha^{13} + \alpha^{12} + \alpha^{12})x + (\alpha^7 + \alpha^{13} + 1)x^2 \\ &\quad + (\alpha^2 + \alpha^7 + \alpha^2)x^3 \\ &= (\alpha^3 + \alpha^3 + 1 + \alpha + \alpha^2) + (1 + \alpha^2 + \alpha^3 + 1 + \alpha + \alpha^2 + \alpha^3 \\ &\quad + 1 + \alpha + \alpha^2 + \alpha^3)x \\ &\quad + (1 + \alpha + \alpha^3 + 1 + \alpha^2 + \alpha^3 + 1)x^2 \\ &\quad + (\alpha^2 + 1 + \alpha + \alpha^3 + \alpha^2)x^3 \\ &= (1 + \alpha + \alpha^2) + (1 + \alpha^2 + \alpha^3)x + (1 + \alpha + \alpha^2)x^2 \\ &\quad + (1 + \alpha + \alpha^3)x^3 \\ &= \alpha^7 x^3 + \alpha^{10} x^2 + \alpha^{13} x + \alpha^{10} \end{aligned}$$

Selesaikan $\sigma(x)s(x) \pmod{(x^4 + \alpha^{14}x^2 + 1)}$,

$$\sigma(x)s(x) = (x^2 + \sigma_1 x + \sigma_0)(\alpha^7 x^3 + \alpha^{10} x^2 + \alpha^{13} x + \alpha^{10})$$

$$\begin{aligned}
&= \alpha^7 x^5 + (\alpha^7 \sigma_1 + \alpha^{10}) x^4 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{13}) x^3 \\
&\quad + (\alpha^{13} \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10}) x^2 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^{13} \sigma_0) x + \alpha^{10} \sigma_0 \\
\sigma(x)s(x) \pmod{(x^4 + \alpha^{14} x^2 + 1)} &= \alpha^7 (\alpha^{14} x^3 + x) + (\alpha^7 \sigma_1 + \alpha^{10}) (\alpha^{14} x^2 + 1) \\
&\quad + \alpha^{14} x^2 + 1) \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{13}) x^3 \\
&\quad + (\alpha^{13} \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10}) x^2 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^{13} \sigma_0) x + \alpha^{10} \sigma_0 \\
&= (\alpha^6 x^3 + \alpha^7 x) + (\alpha^6 \sigma_1 x^2 + \alpha^7 \sigma_1 + \alpha^9 x^2 + \alpha^{10}) \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{13}) x^3 \\
&\quad + (\alpha^{13} \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10}) x^2 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^{13} \sigma_0) x + \alpha^{10} \sigma_0 \\
&= (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{13} + \alpha^6) x^3 \\
&\quad + (\alpha^{13} \sigma_1 + \alpha^6 \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10} \\
&\quad + \alpha^9) x^2 + (\alpha^{10} \sigma_1 + \alpha^{13} \sigma_0 + \alpha^7) x \\
&\quad + (\alpha^7 \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10})
\end{aligned}$$

Kemudian substitusikan persamaan di atas ke

$$\sigma(x)s(x) \equiv \sigma'(x) \pmod{(x^4 + \alpha^{14} x^2 + 1)}$$

Oleh karena itu, perlu menyelesaikan sistem persamaan berikut untuk mendapatkan nilai dari σ_1 dan σ_0 .

$$\begin{cases} \alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{13} + \alpha^6 = 0 \\ \alpha^{10} \sigma_1 + \alpha^{13} \sigma_0 + \alpha^7 = 0 \end{cases}$$

Didapatkan $\sigma_0 = \alpha^4$ dan $\sigma_1 = \alpha^2$, sehingga

$$\sigma(x) = x^2 + \alpha^2 x + \alpha^4 = (x + \alpha^7)(x + \alpha^{12})$$

Karena $\alpha_6 = \alpha^7$ dan $\alpha_{11} = \alpha^{12}$, maka diperoleh himpunan lokasi *error*nya adalah

$$B = \{i \mid \sigma(\alpha_i) = 0\} = \{6, 11\}$$

Sehingga dapat ditemukan vektor *error* $e' = [0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0]$, kemudian

$$Y'_7 = Y_7 - e' = [0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1]$$

Setelah Y_7 dikoreksi didapatkan Y'_7 dan karena Y'_7 dihasilkan dari *standard form generator matriks* yang mana 4 bit dari kiri merupakan pesan informasi atau data bit, dan 8 bit dari kanan merupakan *parity* bit. Maka dapat diambil 4 bit *binary* Y'_7 dari kiri.

$$\hat{m}_7 = [0 \ 0 \ 0 \ 1]$$

h. Cari sindrom $s(x)$ dari

$$Y_8 = C'_8 \times P^{-1} = [0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1]$$

$$\begin{aligned} s(x) &= \sum_{i=1}^{12} \frac{y_i}{x - \alpha_i} \\ &= \frac{1}{x - \alpha^5} + \frac{1}{x - \alpha^6} + \frac{1}{x - \alpha^{13}} \\ &= (\alpha^3 + \alpha^3 + \alpha^{10}) + (\alpha^{13} + \alpha^{12} + \alpha^{12})x + (\alpha^7 + \alpha^{13} + 1)x^2 \\ &\quad + (\alpha^2 + \alpha^7 + \alpha^2)x^3 \\ &= (\alpha^3 + \alpha^3 + 1 + \alpha + \alpha^2) + (1 + \alpha^2 + \alpha^3 + 1 + \alpha + \alpha^2 + \alpha^3 \\ &\quad + 1 + \alpha + \alpha^2 + \alpha^3)x \\ &\quad + (1 + \alpha + \alpha^3 + 1 + \alpha^2 + \alpha^3 + 1)x^2 \\ &\quad + (\alpha^2 + 1 + \alpha + \alpha^3 + \alpha^2)x^3 \end{aligned}$$

$$\begin{aligned}
&= (1 + \alpha + \alpha^2) + (1 + \alpha^2 + \alpha^3)x + (1 + \alpha + \alpha^2)x^2 \\
&\quad + (1 + \alpha + \alpha^3)x^3 \\
&= \alpha^7 x^3 + \alpha^{10} x^2 + \alpha^{13} x + \alpha^{10}
\end{aligned}$$

Selesaikan $\sigma(x)s(x) \pmod{(x^4 + \alpha^{14}x^2 + 1)}$,

$$\begin{aligned}
\sigma(x)s(x) &= (x^2 + \sigma_1 x + \sigma_0)(\alpha^7 x^3 + \alpha^{10} x^2 + \alpha^{13} x + \alpha^{10}) \\
&= \alpha^7 x^5 + (\alpha^7 \sigma_1 + \alpha^{10})x^4 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{13})x^3 \\
&\quad + (\alpha^{13} \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10})x^2 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^{13} \sigma_0)x + \alpha^{10} \sigma_0 \\
\sigma(x)s(x) \pmod{(x^4 + \alpha^{14}x^2 + 1)} &= \alpha^7(\alpha^{14}x^3 + x) + (\alpha^7 \sigma_1 + \alpha^{10})(\alpha^{14}x^2 + 1) \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{13})x^3 \\
&\quad + (\alpha^{13} \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10})x^2 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^{13} \sigma_0)x + \alpha^{10} \sigma_0 \\
&= (\alpha^6 x^3 + \alpha^7 x) + (\alpha^6 \sigma_1 x^2 + \alpha^7 \sigma_1 + \alpha^9 x^2 + \alpha^{10}) \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{13})x^3 \\
&\quad + (\alpha^{13} \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10})x^2 \\
&\quad + (\alpha^{10} \sigma_1 + \alpha^{13} \sigma_0)x + \alpha^{10} \sigma_0 \\
&= (\alpha^{10} \sigma_1 + \alpha^7 \sigma_0 + \alpha^{13} + \alpha^6)x^3 \\
&\quad + (\alpha^{13} \sigma_1 + \alpha^6 \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10} \\
&\quad + \alpha^9)x^2 + (\alpha^{10} \sigma_1 + \alpha^{13} \sigma_0 + \alpha^7)x \\
&\quad + (\alpha^7 \sigma_1 + \alpha^{10} \sigma_0 + \alpha^{10})
\end{aligned}$$

Kemudian substitusikan persamaan di atas ke

$$\sigma(x)s(x) \equiv \sigma'(x) \pmod{(x^4 + \alpha^{14}x^2 + 1)}$$

Oleh karena itu, perlu menyelesaikan sistem persamaan berikut untuk mendapatkan nilai dari σ_1 dan σ_0 .

$$\begin{cases} \alpha^{10}\sigma_1 + \alpha^7\sigma_0 + \alpha^{13} + \alpha^6 = 0 \\ \alpha^{10}\sigma_1 + \alpha^{13}\sigma_0 + \alpha^7 = 0 \end{cases}$$

Didapatkan $\sigma_0 = \alpha^4$ dan $\sigma_1 = \alpha^2$, sehingga

$$\sigma(x) = x^2 + \alpha^2x + \alpha^4 = (x + \alpha^7)(x + \alpha^{12})$$

Karena $\alpha_6 = \alpha^7$ dan $\alpha_{11} = \alpha^{12}$, maka diperoleh himpunan lokasi *error*nya adalah

$$B = \{i \mid \sigma(\alpha_i) = 0\} = \{6, 11\}$$

Sehingga dapat ditemukan vektor *error* $e' = [0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0]$, kemudian

$$Y'_8 = Y_8 - e' = [0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1]$$

Setelah Y_8 dikoreksi didapatkan Y'_8 dan karena Y'_8 dihasilkan dari *standard form generator matriks* yang mana 4 bit dari kiri merupakan pesan informasi atau data bit, dan 8 bit dari kanan merupakan *parity* bit. Maka dapat diambil 4 bit *binary* Y'_8 dari kiri.

$$\hat{m}_8 = [0 \ 0 \ 0 \ 1]$$

Setelah kita mendapatkan semua kata kode yang telah dikoreksi, langkah terakhir adalah mengalikan \hat{m}_i dengan S^{-1} untuk memperoleh pesan asli sebagai berikut:

$$m'_1 = [1 \ 1 \ 0 \ 0] \times \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} = [0 \ 1 \ 0 \ 0]$$

$$m'_2 = [1 \ 0 \ 0 \ 0] \times \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} = [1 \ 0 \ 1 \ 1]$$

$$m'_3 = [1 \ 1 \ 0 \ 0] \times \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} = [0 \ 1 \ 0 \ 0]$$

$$m'_4 = [1 \ 1 \ 0 \ 1] \times \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} = [0 \ 0 \ 0 \ 1]$$

$$m'_5 = [1 \ 1 \ 0 \ 0] \times \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} = [0 \ 1 \ 0 \ 0]$$

$$m'_6 = [0 \ 1 \ 1 \ 1] \times \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} = [1 \ 1 \ 0 \ 1]$$

$$m'_7 = [0 \ 0 \ 0 \ 1] \times \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} = [0 \ 1 \ 0 \ 1]$$

$$m'_8 = [0 \ 0 \ 0 \ 1] \times \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} = [0 \ 1 \ 0 \ 1]$$

Berdasarkan proses dekripsi di atas diperoleh *codeword* yaitu 01001011010000010100110101010101. Untuk mengembalikan kedalam bentuk teks, perlu membagi pesan biner tersebut ke dalam blok-blok dengan panjang 8-bit. Berdasarkan tabel ASCII didapatkan 01001011010000010100110101010101 = KAMU.

4.4 Analisis Hasil

Berdasarkan pembentukan kunci pada algoritma McEliece, kunci publik G' dengan ukuran 12×4 telah berhasil dibentuk dengan langkah-langkah yang kompleks dan kuat. Pada tahap awal melibatkan algoritma decoding, dalam hal ini menggunakan metode kode Goppa untuk menentukan parameter kunci n dan k . Proses ini penting sebagai dasar keamanan sistem kriptografi McEliece. Algoritma decoding menghasilkan matriks generator G , yang berfungsi sebagai dasar untuk pembangkitan matriks acak S dan matriks permutasi P di mana penggunaan matriks acak ini menciptakan kekacauan struktural yang meningkatkan keamanan kunci publik.

Proses enkripsi pada kriptosistem McEliece membuktikan bahwa sistem ini dapat melindungi dan menjaga kerahasiaan informasi sensitif. Pada tahap awal, pesan teks dikonversikan menjadi representasi biner dengan panjang 8 bit yang kemudian dibagi ke dalam blok-blok dengan panjang 4 bit. Pesan ini kemudian dikalikan dengan matriks generator G' sebagai kunci publik menjadikannya sulit terbaca oleh pihak yang tidak berhak. Proses penggabungan *error* acak ke setiap blok *ciphertext* menambah tingkat keamanan, sehingga proses enkripsi menjadi langkah penting dalam melindungi kerahasiaan pesan dalam sistem kriptografi McEliece.

Proses dekripsi dan pengkoreksian error pada algoritma McEliece dengan kode Goppa terdapat beberapa langkah untuk mengembalikan pesan terekripsi ke bentuk semula. Setelah menerima *ciphertext*, langkah awal adalah mengidentifikasi matriks invers P dan S yang sebelumnya digunakan dalam proses pembentukan kunci. Pada proses dekripsi, langkah pertama adalah mengalikan setiap blok pesan

terenkripsi dengan matriks invers P untuk mendapatkan vektor sindrom. Kemudian, sindrom dihitung dengan mengalikan vektor tersebut dengan matriks *parity check* kode Goppa. Sindrom ini mencerminkan pola *error* dalam pesan yang terenkripsi dan digunakan untuk mendeteksi *error* melalui algoritma koreksi *error* pada kode Goppa yang membantu menemukan polinomial lokasi *error*-nya. Polinomial ini memiliki akar-akar yang menunjukkan posisi bit-bit yang salah dalam vektor biner. Setelah lokasi *error* ditemukan, *error* dikoreksi dengan menambahkan bit yang terdeteksi. Selanjutnya, hasil dikalikan dengan matriks invers S untuk mendapatkan pesan asli. Hasil *binary* dikembalikan ke bentuk teks berdasarkan tabel ASCII.

4.5 Kajian Integrasi Agama

Berdasarkan hasil dari pembahasan diatas didapatkan kesimpulan bahwa, enkripsi dan dekripsi pesan menggunakan kriptosistem McEliece ini memastikan bahwa pesan hanya dapat diakses oleh penerima yang berhak, tanpa resiko modifikasi atau penyalahgunaan. Prinsip menjaga amanah dan keutuhan pesan ini mencerminkan nilai-nilai keagamaan tentang kejujuran dan tanggung jawab dalam menyampaikan informasi. Amanah bukan hanya sekedar menjaga barang fisik tetapi juga informasi yang bersifat pribadi dan rahasia. Penggunaan kriptografi, seperti kode goppa pada kriptosistem McEliece merupakan bentuk konkret dari upaya menjaga amanah dengan melindungi informasi dari pihak yang tidak berwenang.

Dalam Al-Qur'an, Allah SWT berfirman:

وَالَّذِينَ هُمْ لِأَمْتِهِمْ وَعَهْدِهِمْ رَاعُونَ ﴿٨﴾

Artinya: “(sesungguhnya beruntung pula) orang-orang yang memelihara amanat (yang dipikulnya) dan janjinya.” (Q.S Al-Mu’minun: 8)

Prinsip menjaga amanat dan integritas informasi sangat relevan dengan nilai yang diajarkan dalam ayat tersebut. Kriptografi tidak hanya melibatkan aspek teknis tetapi juga mengandung nilai etika dan moral dalam penerapannya. Memastikan bahwa pesan tetap rahasia dan tidak disalahgunakan adalah bentuk tanggung jawab yang harus diemban oleh setiap individu yang terlibat dalam pengelolaan informasi.

Amanah dalam islam adalah tentang menjaga kepercayaan dan bertindak jujur. Dengan menggunakan kode goppa dalam kriptosistem McEliece, kita berupaya memastikan bahwa setiap informasi yang dikirim dan diterima tetap utuh dan rahasia, mencerminkan kejujuran dalam mengelola data. Seperti sabda rosulullah SAW:

أَدِّ الْأَمَانَةَ إِلَى مَنْ أَيْتَمَّنَكَ وَلَا تَخُنْ مَنْ خَانَ

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

Dengan mengintegrasikan nilai-nilai yang diajarkan oleh nabi muhammad SAW dalam hadis ini, kita dapat memahami bahwa teknologi dan etika tidaklah terpisah. Melalui penggunaan kriptografi yang kuat seperti kode Goppa dalam kriptosistem McEliece, kita tidak hanya memenuhi tuntutan teknis tetapi juga menjalankan amanah dengan penuh tanggung jawab sesuai dengan ajaran islam. Ini memastikan bahwa kita menjaga kepercayaan, melindungi kerahasiaan, dan bertindak dengan adil dalam setiap tindakan sesuai dengan prinsip-prinsip kejujuran dan integritas yang diajarkan oleh nabi muhammad SAW.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan dari pembahasan di atas didapatkan kesimpulan bahwa

1. Implementasi kode Goppa pada kriptosistem McEliece dengan menggunakan polinomial $g(x) = x^2 + \alpha^7x + 1$ pada $GF(2^4)$ didapatkan parameter kode Goppa dengan panjang $n = 12$ dan dimensi kode $k = 4$ dengan tingkat kesalahan $t = 2$ menunjukkan teknik pengkodean klasik dapat digunakan untuk proses enkripsi pada kriptografi modern. Kunci publik G' dan kunci privat P dan S , dibangkitkan berdasarkan matriks kode Goppa dengan kunci publik yang berfungsi untuk mengenkripsi pesan dan kunci privat untuk dekripsi.
2. Enkripsi pesan dilakukan dengan cara mengalikan pesan m_i yang sudah dipilih dengan kunci publik G' , kemudian penambahan *error* e pada pesan m_i yang telah dikalikan dengan kunci publik G' , menciptakan *ciphertext* yang menyulitkan untuk dekripsi tanpa kunci privat. Penambahan *error* acak ini memberikan keamanan tambahan, yang menjadikan proses enkripsi sebagai langkah penting dalam menjaga kerahasiaan dan keamanan pesan.
3. Proses dekripsi dilakukan dengan menggunakan kunci privat yang terdiri dari matriks permutasi dan matriks paritas yang sesuai kode Goppa. Kode Goppa digunakan untuk menghitung *syndrome* $s(x)$, yang mendeteksi *error* dan menentukan lokasi bit yang salah. Proses koreksi *error* ini memungkinkan penerima untuk memulihkan pesan asli. Sehingga, Dengan memanfaatkan

polinomial untuk menentukan parameter kode memberikan kemampuan koreksi *error* yang tinggi, sehingga membuat sistem lebih sulit untuk dipecahkan oleh algoritma serangan yang berbasis kuantum. Dengan mengimplementasikan kode Goppa dalam kriptosistem McEliece menunjukkan bahwa sistem ini dapat meningkatkan keamanan pertukaran informasi dan menangani ancaman dari komputer kuantum.

5.2 Saran

Saran untuk penelitian selanjutnya, diharapkan dapat melakukan pengamanan pertukaran data dalam bentuk gambar, audio, ataupun video dengan menggunakan algoritma McEliece yang menggunakan kode Goppa sebagai koreksi *error*.

DAFTAR PUSTAKA

- Abidin , Z., & Khairudin, F. (2017). Penafsiran Ayat-ayat Amanah dalam Al-Qur'an. *Jurnal Syahadah*, 120-144.
- Al Albani, M. N. (2007). *Mukhtashar Shahih Bukhari*. Pustaka Azzam.
- Andika, T., Taquyuddin, M., & Admizal, I. (2020). Amanah Dan Khianat Dalam Al-Qur'an Menurut Quraish Shihab. *Al Tadabbur: Jurnal Ilmu Alquran Dan Tafsir*, 177-206.
- Anggraeni, W. (2004). Deteksi Dan Koreksi Kesalahan Informasi Dalam Sandi Biner Dengan Menggunakan Metode Hamming. *JUTI*, 3, 101-108.
- Ariyus , D. (2008). *Pengantar Ilmu Kriptografi*. Yogyakarta: ANDI.
- Artin, M. (1991). *Algebra*. Englewood Cliffs (New Jersey): Prentice Hall.
- Burton , D. M. (2011). *Elementary Number Theory* (7th ed.). (S. K. Mattson , Ed.) New York: McGraw-Hill.
- Chen, B., & Zhang, G. (2023). *The number of extended irreducible binary Goppa codes*. China: IEEE Transactions on Information Theory.
- Childs, L. N. (2019). *Cryptography and Error Correction*. New York: Springer International Publishing.
- Halim, A., & Zulheldi. (2019). Karakteristik Pemegang Amânah dalam Al-Qur'an. *MASHDAR:Jurnal Studi al-Qur'an dan Hadis*, 185-198.
- Indrayani, L. A., & Suartana, I. M. (2019). Implementasi Kriptografi dengan Modifikasi Algoritma Advanced Encryption Standard (AES) untuk Pengamanan File Document. *JINACS : (Journal of Informatics and Computer Science)*.
- Irawan, W. H., Hijriyah, N., & Habibi, A. R. (2014). *Teori Bilangan*. Malang: UIN Maliki Press.
- Kemenag RI. (2024). *Qur'an Kemenag*. Jakarta Timur : Lajnah Pentashihan Mushaf Al-Qur'an. Retrieved from <https://quran.kemenag.co.id>
- Lapele, D. A. (2023). *Teori Bilangan* . Bandung: Widina Bhakti Persada Bandung.
- Ling, S., & Xing, C. (2004). *Coding Theory*. New York: Cambridge University Press.
- Munir , R. (2008). *Matematika Diskrit* . Bandung : Informatika.
- Niven, I., Zuckerman, H. S., & Montgomery, H. L. (1980). *An Introduction to the Theory of Numbers* (Fifth edition ed.). New York: John Wiley and Sons, 1991.

- Prayitno, A., & Nurdin. (2017). Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia Menggunakan Algoritma Cipher Transposition. *JESIK: Jurnal Elektronik Sistem Informasi dan Komputer*, 3.
- Rosdiana. (2015). Sekuritas Sistem Dengan Kriptografi. *al-Khwarizmi*, 21-32.
- Sadikin , R. (2012). *Kriptografi untuk Keamanan Jaringan*. Yogyakarta: C.V. ANDI OFFSET.
- Sahri. (2018). Penafsiran Ayat-Ayat Al-Qur'an Tentang Amanah Menurut M. Quraish Shihab. *Jurnal Madaniyah*, 8, 125-140.
- Shihab , M. Q. (2002). *Tafsir Al-Misbah* (Vol. Vol.2). Jakarta: Lentera Hati.
- Siim, S. (2015). Study of McEliece Cryptosystem. *Research Seminar in Seminar Cryptography*.
- Singh, H. (2020). *Code based Cryptography: Classic McEliece*.
- Stallings, W. (2003). *Cryptography and Network Security*. New Jersey: Pearson Education.
- Sukirman. (2016). *Teori bilangan*. jakarta: Universitas terbuka.
- Surnawani, Jarkasih, S., & Fatimah, U. (2022). Penggunaan Public Key Infrastructure Kunci Persetujuan (Key Agreement). *TripleA : Jurnal Pendidikan Teknologi Informasi* , 97-102.
- Waliprana, W. E. (2011). *Studi dan Implementasi Algoritma kunci publik McEliece*. Bandung: Makalah, Institut Teknologi Bandung.
- Ziaurrahman, M., Utami, E., & Wibowo, F. W. (2019). Modifikasi Kriptografi Klasik Vigenere Cipher Menggunakan One Time Pad Dengan Enkripsi Berlanjut. *Jurnal Informasi Interaktif*, Vol.4.

LAMPIRAN

Lampiran 1. Pesan asli dengan daftar simbol dan kode biner berdasarkan tabel ASCII.

Pesan	Hari lahirnya bangsa Indonesia				
Simbol	Kode Biner	Simbol	Kode Biner	Simbol	Kode Biner
H	01001000	n	01101110	I	01001001
a	01100001	y	01111001	n	01101110
r	01110010	a	01100001	d	01100100
i	01101001	b	01100010	o	01101111
l	01101100	a	01100001	n	01101110
a	01100001	n	01101110	e	01100101
h	01101000	g	01100111	s	01110011
i	01101001	s	01110011	i	01101001
r	01110010	a	01100001	a	01100001

Lampiran 2. Hasil program *sagemath* untuk implementasi algoritma kriptosistem McEliece menggunakan kode Goppa $n = 12$ dan $k = 4$.

Kunci	
$G_{4 \times 12}$	$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$
$S_{4 \times 4}$	$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

$P_{12 \times 12}$	$\begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$											
$G' = SGP$	$\begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$											
Pesan	Codeword				Pesan	Codeword						
m_1	0100				m_{28}	0001						
m_2	1000				m_{29}	0110						
m_3	0110				m_{30}	1110						
m_4	0001				m_{31}	0110						
m_5	0111				m_{32}	0111						
m_6	0010				m_{33}	0111						
m_7	0110				m_{34}	0011						
m_8	1001				m_{35}	0110						
m_9	0110				m_{36}	0001						
m_{10}	1100				m_{37}	0100						
m_{11}	0110				m_{38}	1001						
m_{12}	0001				m_{39}	0110						
m_{13}	0110				m_{40}	1110						
m_{14}	1000				m_{41}	0110						
m_{15}	0110				m_{42}	0100						
m_{16}	1001				m_{43}	0110						
m_{17}	0111				m_{44}	1111						

m_{18}	0010	m_{45}	0110
m_{19}	0110	m_{46}	1110
m_{20}	1110	m_{47}	0110
m_{21}	0111	m_{48}	0101
m_{22}	1001	m_{49}	0111
m_{23}	0110	m_{50}	0011
m_{24}	0001	m_{51}	0110
m_{25}	0110	m_{52}	1001
m_{26}	0010	m_{53}	0110
m_{27}	0110	m_{54}	0001
Proses Enkripsi			
e	000000001001		
Pesan	$C'_i = m_i G' + e$		Cipherteks
m_1	001111111010		C'_1
m_2	010010101100		C'_2
m_3	100001011100		C'_3
m_4	100010010011		C'_4
m_5	000011000110		C'_5
m_6	101110101111		C'_6
m_7	100001011100		C'_7
m_8	110000110110		C'_8
m_9	100001011100		C'_9
m_{10}	011101011111		C'_{10}
m_{11}	100001011100		C'_{11}
m_{12}	100010010011		C'_{12}
m_{13}	100001011100		C'_{13}
m_{14}	010010101100		C'_{14}
m_{15}	100001011100		C'_{15}
m_{16}	001100101011		C'_{16}

m_{17}	000011000110	C'_{17}
m_{18}	101110101111	C'_{18}
m_{19}	100001011100	C'_{19}
m_{20}	110011111001	C'_{20}
m_{21}	000011000110	C'_{21}
m_{22}	110000110110	C'_{22}
m_{23}	100001011100	C'_{23}
m_{24}	100010010011	C'_{24}
m_{25}	100001011100	C'_{25}
m_{26}	101110101111	C'_{26}
m_{27}	100001011100	C'_{27}
m_{28}	100010010011	C'_{28}
m_{29}	100001011100	C'_{29}
m_{30}	110011111001	C'_{30}
m_{31}	100001011100	C'_{31}
m_{32}	000011000110	C'_{32}
m_{33}	000011000110	C'_{33}
m_{34}	001100110101	C'_{34}
m_{35}	100001011100	C'_{35}
m_{36}	100010010011	C'_{36}
m_{37}	001111111010	C'_{37}
m_{38}	110000110110	C'_{38}
m_{39}	100001011100	C'_{39}
m_{40}	110011111001	C'_{40}
m_{41}	100001011100	C'_{41}
m_{42}	001111111010	C'_{42}
m_{43}	100001011100	C'_{43}
m_{44}	010001100011	C'_{44}
m_{45}	100001011100	C'_{45}
m_{46}	110011111001	C'_{46}

m_{47}	100001011100	C'_{47}
m_{48}	101101100000	C'_{48}
m_{49}	000011000110	C'_{49}
m_{50}	001100110101	C'_{50}
m_{51}	100001011100	C'_{51}
m_{52}	110000110110	C'_{52}
m_{53}	100001011100	C'_{53}
m_{54}	100010010011	C'_{54}
Proses Dekripsi		
Cipherteks	$Y_i = C'_i \times P^{-1}$	
C'_1	111011000111	
C'_2	001011101000	
C'_3	010101100001	
C'_4	000110010011	
C'_5	010010100010	
C'_6	101111110110	
C'_7	010101100001	
C'_8	001100101011	
C'_9	010101100001	
C'_{10}	110001111111	
C'_{11}	010101100001	
C'_{12}	000110010011	
C'_{13}	010101100001	
C'_{14}	001011101000	
C'_{15}	010101100001	
C'_{16}	001100101011	
C'_{17}	010010100010	
C'_{18}	101111110110	
C'_{19}	010101100001	

C'_{20}	01111011001
C'_{21}	010010100010
C'_{22}	001100101011
C'_{23}	010101100001
C'_{24}	000110010011
C'_{25}	010101100001
C'_{26}	10111110110
C'_{27}	010101100001
C'_{28}	000110010011
C'_{29}	010101100001
C'_{30}	01111011001
C'_{31}	01010110001
C'_{32}	010010100010
C'_{33}	010010100010
C'_{34}	101000110101
C'_{35}	010101100001
C'_{36}	000110010011
C'_{37}	111011000111
C'_{38}	001100101011
C'_{39}	010101100001
C'_{40}	01111011001
C'_{41}	010101100001
C'_{42}	111011000111
C'_{43}	010101100001
C'_{44}	011000011010
C'_{45}	010101100001
C'_{46}	01111011001
C'_{47}	010101100001
C'_{48}	111100000100
C'_{49}	010010100010

C'_{50}	101000110101		
C'_{51}	010101100001		
C'_{52}	001100101011		
C'_{53}	010101100001		
C'_{54}	000110010011		
Cipherteks	Decoding (\hat{m}_i)	$m_i = \hat{m}_i \times S^{-1}$	Pesan
C'_1	1110	0100	m_1
C'_2	0010	1000	m_2
C'_3	0101	0110	m_3
C'_4	0001	0001	m_4
C'_5	0100	0111	m_5
C'_6	1011	0010	m_6
C'_7	0101	0110	m_7
C'_8	0011	1001	m_8
C'_9	0101	0110	m_9
C'_{10}	1100	1100	m_{10}
C'_{11}	0101	0110	m_{11}
C'_{12}	0001	0001	m_{12}
C'_{13}	0101	0110	m_{13}
C'_{14}	0010	1000	m_{14}
C'_{15}	0101	0110	m_{15}
C'_{16}	0011	1001	m_{16}
C'_{17}	0100	0111	m_{17}
C'_{18}	1011	0010	m_{18}
C'_{19}	0101	0110	m_{19}
C'_{20}	0111	1110	m_{20}
C'_{21}	0100	0111	m_{21}
C'_{22}	0011	1001	m_{22}
C'_{23}	0101	0110	m_{23}

C'_{24}	0001	0001	m_{24}
C'_{25}	0101	0110	m_{25}
C'_{26}	1011	0010	m_{26}
C'_{27}	0101	0110	m_{27}
C'_{28}	0001	0001	m_{28}
C'_{29}	0101	0110	m_{29}
C'_{30}	0111	1110	m_{30}
C'_{31}	0101	0110	m_{31}
C'_{32}	0100	0111	m_{32}
C'_{33}	0100	0111	m_{33}
C'_{34}	1010	0011	m_{34}
C'_{35}	0101	0110	m_{35}
C'_{36}	0001	0001	m_{36}
C'_{37}	1110	0100	m_{37}
C'_{38}	0011	1001	m_{38}
C'_{39}	0101	0110	m_{39}
C'_{40}	0111	1110	m_{40}
C'_{41}	0101	0110	m_{41}
C'_{42}	1110	0100	m_{42}
C'_{43}	0101	0110	m_{43}
C'_{44}	0110	1111	m_{44}
C'_{45}	0101	0110	m_{45}
C'_{46}	0111	1110	m_{46}
C'_{47}	0101	0110	m_{47}
C'_{48}	1111	0101	m_{48}
C'_{49}	0100	0111	m_{49}
C'_{50}	1010	0011	m_{50}
C'_{51}	0101	0110	m_{51}
C'_{52}	0011	1001	m_{52}
C'_{53}	0101	0110	m_{53}

C'_{54}	0001	0001	m_{54}
-----------	------	------	----------

Pesan	<i>Codeword</i>	Kode Biner	Simbol
m_1	0100	01001000	H
m_2	1000		
m_3	0110	01100001	a
m_4	0001		
m_5	0111	01110010	r
m_6	0010		
m_7	0110	01101001	i
m_8	1001		
m_9	0110	01101100	l
m_{10}	1100		
m_{11}	0110	01100001	a
m_{12}	0001		
m_{13}	0110	01101000	h
m_{14}	1000		
m_{15}	0110	01101001	i
m_{16}	1001		
m_{17}	0111	01110010	r
m_{18}	0010		
m_{19}	0110	01101110	n
m_{20}	1110		
m_{21}	0111	01111001	y
m_{22}	1001		
m_{23}	0110	01100001	a
m_{24}	0001		
m_{25}	0110	01100010	b
m_{26}	0010		
m_{27}	0110	01100001	a

m_{28}	0001		
m_{29}	0110	01101110	n
m_{30}	1110		
m_{31}	0110	01100111	g
m_{32}	0111		
m_{33}	0111	01110011	s
m_{34}	0011		
m_{35}	0110	01100001	a
m_{36}	0001		
m_{37}	0100	01001001	l
m_{38}	1001		
m_{39}	0110	01101110	n
m_{40}	1110		
m_{41}	0110	01100100	d
m_{42}	0100		
m_{43}	0110	01101111	o
m_{44}	1111		
m_{45}	0110	01101110	n
m_{46}	1110		
m_{47}	0110	01100101	e
m_{48}	0101		
m_{49}	0111	01110011	s
m_{50}	0011		
m_{51}	0110	01101001	i
m_{52}	1001		
m_{53}	0110	01100001	a
m_{54}	0001		
Pesan yang diperoleh		Hari lahirnya bangsa Indonesia	

RIWAYAT HIDUP



Lili Khoiriyah, lahir di Oku Timur pada 29 September 2002. Penulis merupakan anak kedua dari dua bersaudara dari Bapak Mahmudin dan Ibu Jamilah. Selama masa pendidikan, penulis menempuh pendidikan mulai dari pendidikan dasar di MI Nurul Ulum Yosowinangun, Sumatera Selatan yang lulus pada tahun 2014. Selanjutnya penulis menempuh pendidikan menengah pertama di SMP Asshiddiqiyah 9 Lampung Tengah dan lulus pada tahun 2017, kemudian melanjutkan pendidikan jenjang menengah atas di SMA A. Wahid Hasyim Tebuireng, Jombang tahun 2020. Setelah lulus dari jenjang menengah atas, pada tahun yang sama penulis melanjutkan pendidikan sebagai mahasiswa program studi Matematika di Universitas Islam Negeri Maulana Malik Ibrahim Malang.

Selama menempuh pendidikan tinggi, penulis turut berkontribusi aktif dalam beberapa kepanitiaan internal kampus seperti PBAK-F dan lainnya. Di luar kampus, Penulis juga berkontribusi aktif dalam organisasi daerah Sumatera Selatan dan menjabat sebagai sekertaris tahun 2022 hingga 2023. Selain itu, penulis juga aktif sebagai anggota Kopma Padang Bulan UIN Malang.



BUKTI KONSULTASI SKRIPSI

Nama : Lili Khoiriyah
NIM : 200601110024
Fakultas/Jurusan : Sains dan Teknologi/Matematika
Judul Skripsi : Implementasi Kode Goppa pada Kriptosistem McEliece
Pembimbing I : Muhammad Khudzaifah, M.Si.
Pembimbing II : Erna Herawati, M.Pd.

No	Tanggal	Hal	Tanda Tangan
1.	9 Januari 2024	Konsultasi Bab I, II, dan III	1.
2.	11 Januari 2024	Konsultasi Kajian Agama	2.
3.	15 Januari 2024	Konsultasi Revisi Kajian Agama	3.
4.	23 Januari 2024	ACC Kajian Agama Bab I dan II	4.
5.	29 Januari 2024	Konsultasi Revisi Bab III	5.
6.	19 Februari 2024	ACC Bab I, II, dan III	6.
7.	26 Februari 2024	ACC Seminar Proposal	7.
8.	28 Maret 2024	Konsultasi Revisi Seminar Proposal	8.
9.	5 Juni 2024	Konsultasi Bab IV	9.
10.	11 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.	10 September 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.	30 September 2024	Konsultasi Revisi Seminar Hasil	16.
17.	21 Oktober 2024	ACC Matriks Revisi Seminar Hasil	17.
18.	21 Oktober 2024	ACC Sidang Skripsi	18.
19.	11 Desember 2024	ACC Keseluruhan	19.

Malang, 11 Desember 2024

Mengetahui,

Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc.

NIP. 19741129 200012 2 005