

**IMPLEMENTASI KODE GOPPA BINER PADA KRIPTOSISTEM
*NIEDERREITER***

SKRIPSI

**OLEH:
ALDINA LAILI CHUSNIA
NIM. 200601110006**



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

**IMPLEMENTASI KODE GOPPA BINER PADA KRIPTOSISTEM
*NIEDERREITER***

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
ALDINA LAILI CHUSNIA
NIM. 200601110006**

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

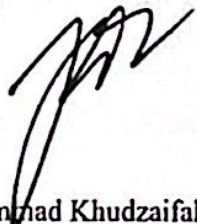
**IMPLEMENTASI KODE GOPPA BINER PADA KRIPTOSISTEM
NIEDERREITER**

SKRIPSI

**Oleh
Aldina Laili Chusnia
NIM. 200601110006**

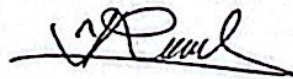
**Telah Disetujui Untuk Diuji
Malang, 10 Desember 2024**

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 BINER PADA KRIPTOSISTEM
NIEDERREITER**

SKRIPSI

Oleh
Aldina Laili Chusnia
NIM. 200601110006

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

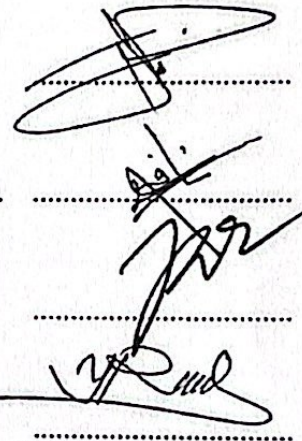
Tanggal, 18 Desember 2024

Ketua Penguji : Hisyam Fahmi, M.Kom.

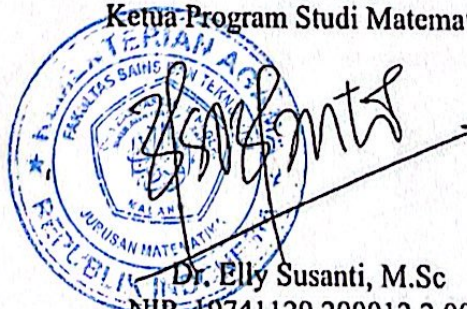
Anggota Penguji 1 : Mohammad Nafie Jauhari, M.Si.

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 : Aldina Laili Chusnia

NIM : 200601110006

Program Studi : Matematika

Fakultas : Sains dan Teknologi

Judul skripsi : Implementasi Kode Goppa Biner pada Kriptosistem *Niederreiter*

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

Malang, 18 Desember 2024



Aldina Laili Chusnia

NIM. 200601110006

MOTO

“Mengalir bersama waktu, menerima setiap liku”

PERSEMBAHAN

Skripsi ini penulis persembahkan kepada:

Ayah Pujiono dan Ibu Painah Wati yang senantiasa mendoakan dan memberi motivasi, nasihat, serta dukungan kepada penulis terhadap setiap langkahnya.
Kakak Nurul Khoiriyah yang memberikan doa dan dukungan kepada penulis.
Serta teman-teman yang selalu memberikan bantuan terhadap kesulitan penulis dan selalu memberikan semangat kepada penulis dalam menyelesaikan skripsi ini.

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji syukur kepada Allah Swt atas limpahan rahmat, petunjuk, dan pertolongan-Nya, penulis mampu menyelesaikan penulisan skripsi dengan judul “Implementasi Kode Goppa Biner pada Kriptosistem *Niederreiter*”. Penulisan skripsi ini merupakan salah satu syarat untuk mendapatkan gelar sarjana dalam bidang matematika di Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang.

Dalam penulisan skripsi ini, penulis mengucapkan terima kasih kepada berbagai pihak yang telah memberikan bimbingan dan arahan. Terutama penulis sampaikan kepada:

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, S.Pd., M.Sc, selaku ketua Program Studi Matematika, Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. Bapak Muhammad Khudzaifah., M.Si, selaku dosen pembimbing I yang telah memberikan bimbingan, arahan, nasihat, dukungan, serta perbaikan demi kebaikan penyusunan skripsi ini.
5. Ibu Erna Herawati, M.Pd, selaku dosen pembimbing II yang telah memberikan bimbingan, arahan, nasihat, dukungan, serta perbaikan demi kebaikan penyusunan skripsi.
6. Bapak Hisyam Fahmi, M.Kom., selaku ketua penguji dalam ujian skripsi yang telah memberikan ilmu pengetahuan dan saran yang membangun dalam penyusunan skripsi.
7. Bapak Mohammad Nafie Jauhari, M.Si., selaku anggota penguji 1 dalam ujian skripsi yang telah memberikan ilmu pengetahuan dan saran yang membangun dalam penyusunan skripsi.
8. Segenap civitas akademika Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang,

terutama untuk seluruh dosen Matematika yang telah memberikan banyak ilmu dan bimbingannya.

9. Kepada kedua orang tua, ayah Pujiono dan ibu Painah Wati yang selalu mendoakan, memberikan segala dukungan, motivasi, dan kerja keras untuk memastikan penulis dapat menyelesaikan pendidikan hingga sarjana.
10. Kepada kakak Nurul Khoiriyah, beserta suaminya Helmi Fakhrudin, dan ponakan kecil Haris Fakhrudin dan Hilda IAI, yang selalu mendoakan dan memberikan dukungan penuh kepada penulis, sekaligus nasehat yang membangun sehingga menjadi motivasi bagi penulis dalam menyelesaikan studi ini.
11. Kepada seseorang berinisial “AW”, terima kasih telah menjadi pendengar setia, pemberi semangat, dan dukungan penuh baik secara materiil maupun non-materiil, serta selalu mengingatkan untuk terus memberikan semangat hingga tugas akhir selesai.
12. Sahabat “CUMEL” Ira, Lili, Nanda, dan Afi, terima kasih atas kebersamaan dan dukungan yang tiada henti, baik dalam suka maupun duka, sejak awal perkuliahan hingga penulisan skripsi ini. Semangat dan perhatian kalian sangat berarti bagi penulis.
13. Kepada teman-teman Kriptografi, Anggi, Aam, Lengga, Soviana, yang selalu siap membantu dengan ide, saran, teori, dan dukungan selama penulis menyelesaikan skripsi ini.
14. Kepada teman-teman PKL JAYA, Rifqi dan Iftanul, yang selalu siap membantu dan memberi dukungan selama penulis menyelesaikan skripsi ini.
15. Untuk seluruh dulur-dulur UKM Seni Religius, yang telah memberikan dukungan dan pengalaman berharga bagi penulis dalam menjalani kehidupan kampus.
16. Untuk seluruh sahabat/sahabati Pergerakan Mahasiswa Islam Indonesia Rayon *Pencerahan Galileo*, yang telah memberikan pengalaman berharga bagi penulis dalam menjalani kehidupan kampus.
17. Untuk seluruh mahasiswa “MAHATMA” Matematika angkatan 2020 yang selalu mendukung dan memberikan semangat dalam perjalanan studi

penulis.

18. Serta semua pihak yang selalu mendukung dan memberikan semangat dalam penyusunan proposal skripsi ini.

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

Malang, 18 November 2024

Penulis

DAFTAR ISI

| | |
|--|--------------|
| HALAMAN JUDUL | i |
| HALAMAN PENGANTAR..... | ii |
| HALAMAN PERSETUJUAN | iii |
| HALAMAN PENGESAHAN..... | iv |
| PERNYATAAN KEASLIAN TULISAN | v |
| MOTO..... | vi |
| PERSEMBAHAN..... | vii |
| KATA PENGANTAR..... | viii |
| DAFTAR ISI..... | xi |
| DAFTAR TABEL | xiii |
| DAFTAR GAMBAR..... | xiv |
| DAFTAR LAMPIRAN | xv |
| ABSTRAK | xvi |
| ABSTRACT | xvii |
| مستخلص البحث | xviii |
| BAB I PENDAHULUAN..... | 1 |
| 1.1 Latar Belakang | 1 |
| 1.2 Rumusan Masalah..... | 5 |
| 1.3 Tujuan Penelitian | 6 |
| 1.4 Manfaat Penelitian | 6 |
| 1.5 Batasan Masalah | 6 |
| 1.6 Definisi Istilah..... | 7 |
| BAB II KAJIAN TEORI | 8 |
| 2.1 Teori Pendukung..... | 8 |
| 2.1.1 Aritmatika Modulo | 8 |
| 2.1.2 Kongruensi | 8 |
| 2.1.3 Kode Linear | 10 |
| 2.1.4 Kode Goppa..... | 13 |
| 2.1.5 Encoding Kode Goppa | 16 |
| 2.1.6 Decoding Kode Goppa | 17 |
| 2.1.7 Finite Field (Lapangan Hingga) | 17 |
| 2.1.8 Kriptografi | 22 |
| 2.1.9 Kriptosistem Niederreiter | 26 |
| 2.2 Kajian Integrasi Topik Dengan Al-Qur'an | 27 |
| 2.3 Kajian Topik dengan Teori Pendukung..... | 33 |
| BAB III METODE PENELITIAN | 35 |
| 3.1 Jenis Penelitian | 35 |
| 3.2 Tahapan Penelitian..... | 35 |
| 3.2.1 Proses Pembentukan Kunci | 35 |
| 3.2.2 Proses Enkripsi | 36 |
| 3.2.3 Proses Dekripsi | 36 |
| BAB IV HASIL DAN PEMBAHASAN | 37 |
| 4.1 Proses Pembentukan Kunci | 37 |
| 4.1.1 Proses Simulasi Pembentukan Kunci pada Kriptosistem <i>Niederreiter</i> | 37 |
| 4.2 Proses Enkripsi | 44 |

| | | |
|--------------|--|-----------|
| 4.2.1 | Proses Simulasi Enkripsi dengan Kriptosistem | |
| | <i>Niederreiter</i> | 44 |
| 4.3 | Proses Dekripsi | 46 |
| 4.3.1 | Proses Simulasi Dekripsi dengan Kriptosistem | |
| | <i>Niederreiter</i> | 47 |
| 4.4 | Analisis Hasil | 56 |
| 4.5 | Kajian Integrasi Agama | 58 |
| BAB V | PENUTUP | 61 |
| 5.1 | Kesimpulan | 61 |
| 5.2 | Saran | 62 |
| | DAFTAR PUSTAKA | 63 |
| | LAMPIRAN | 65 |
| | RIWAYAT HIDUP | 72 |

DAFTAR TABEL

| | | |
|------------|--|----|
| Tabel 2.1 | Operasi Penjumlahan..... | 11 |
| Tabel 2.2 | Operasi Kode Linear | 12 |
| Tabel 2.3 | Nilai Vektor dari w | 13 |
| Tabel 2.4 | Operasi Penjumlahan dan Perkalian $GF(24)$ | 22 |
| Tabel 2.5 | Elemen dari $GF(23)$ | 22 |
| Tabel 4. 1 | Representasi Polinomial $GF(24)$ | 38 |

DAFTAR GAMBAR

| | | |
|------------|--|----|
| Gambar 2.1 | (a) Kriptografi Simetris (b) Kriptografi Asimetris. | 25 |
|------------|--|----|

DAFTAR LAMPIRAN

| | | |
|--------------------|--|----|
| Lampiran 1. | Tabel ASCII 8 bit | 65 |
| Lampiran 2. | Pesan asli dengan daftar simbol dan kode biner berdasarkan Tabel ASCII..... | 67 |
| Lampiran 3. | Implementasi kode Goppa biner pada kriptosistem Niederreiter $n = 12$ dan $k = 4$ | 67 |

ABSTRAK

Chusnia, Aldina Laili. 2024. **Implementasi Kode Goppa Biner pada Kriptosistem Niederreiter**. 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 *Niederreiter*, Kriptografi

Dalam perkembangan kriptografi modern, ancaman dari komputer kuantum mendorong kebutuhan proses enkripsi yang lebih kuat. Salah satu metode kriptografi pasca-kuantum yang mampu melindungi data dari ancaman komputer kuantum adalah kriptosistem *Niederreiter* dengan menggunakan kode Goppa biner. Kode Goppa biner digunakan untuk proses pembentukan kunci publik dan kunci privat dan proses *decoding*. Penelitian ini dilakukan dengan memanfaatkan polinomial Goppa $g(x) = x^2 + a^7x + 1$ pada lapangan hingga $GF(2^4)$ yang menghasilkan parameter kode dengan panjang $n = 12$ dan dimensi $k = 4$, dan tingkat kesalahan $t = 2$. Kode Goppa diterapkan pada proses koreksi *error* melalui perhitungan *syndrome* yang memungkinkan deteksi dan perbaikan bit yang salah dan memulihkan pesan asli dengan akurat. Hasil penelitian menunjukkan bahwa kode Goppa biner dapat mendeteksi serta memperbaiki kesalahan, sehingga memastikan integrasi pesan. Penelitian ini diharapkan dapat memberikan kontribusi pada pengembangan kriptosistem untuk menjaga kerahasiaan informasi dalam era digital yang semakin berkembang.

ABSTRACT

Chusnia, Aldina Laili. 2024. **The implementation binary Goppa codes on Niederreiter 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.

Kata Kunci: Goppa Code, Niederreiter Cryptosystem, Cryptography

In terms of modern cryptography development, the threat of quantum computers drives the need for stronger encryption processes. One of the post-quantum cryptography methods that can protect data from the threat of quantum computers is the Niederreiter cryptosystem using binary Goppa codes. The binary Goppa code is used for the formation of public and private keys and the decoding process. This research is conducted by utilizing the Goppa polynomial $g(x) = x^2 + \alpha^7x + 1$ in the finite field $GF(2^4)$ which produces code parameters with length $n = 12$ and dimension $k = 4$, and error rate $t = 2$. The Goppa code is applied to the error correction process through syndrome calculation which enables the detection and correction of erroneous bits and restores the original message accurately. The results show that binary Goppa codes can detect as well as correct errors, thus ensuring message integration. This research is expected to contribute to the development of cryptosystems to maintain information confidentiality in the growing digital era.

مستخلص البحث

حسنا ، الدينا ليلي.٢٠٢٤. تنفيذ شيفرة جوبا الثنائي في نظام التشفير نيديرويتير. البحث الجامعي. قسم الر ضيات ، كلية العلوم والتكنولوجيا، جامعة مولا مالك إبراهيم الإسلامية الحكومية، مالانج. المشرف الأول: محمد حذيفة، الماجستير. المشرفة الثانية: إير هيراواتي، الماجستير.

الكلمات المفتاحية: التشفير جو ، نظام تشفير نيديرويتير، التشفير

في تطوير التشفير الحديث ، تقود تهديد من أجهزة الحواسيب الكمية الحاجة إلى عمليات تشفير أقوى. إحدى طرق التشفير ما بعد الكم القادرة على حماية البيانات من فهدويد الحواسيب الكمية هي نظام التشفير *Niederreiter* استخدام كود *Goppa* الثنائي. يستخدم رمز *Goppa* الثنائي لعملية تشكيل وفك تشفير المفتاح العام والمفتاح الخاص. أجريت هذه الدراسة من خلال استخدام كثيرات حدود $Goppa g(x) = x^2 + a^7x +$ في الحقل إلى $GF(24)$ التي أنتجت معلمات الكود بطول $n = 12$ والبعد $k = 4$ ، ومعدل الخطأ $t = 2$. يتم تطبيق كود *Goppa* على عملية تصحيح الخطأ من خلال حسابات المتلازمة التي تسمح اكتشاف وتصحيح البتات الخاطئة والاسترداد الدقيق للرسالة الأصلية. تظهر النتائج أن رمز *Goppa* الثنائي يمكنه اكتشاف الأخطاء وتصحيحها ، و لتالي ضمان تكامل الرسائل. من المتوقع أن يساهم هذا البحث في تطوير أنظمة التشفير للحفاظ على سرية المعلومات في العصر الرقمي المتطور بشكل متزايد.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada masa digital yang semakin maju, komunikasi telah menjadi aspek penting dalam berbagai kehidupan. Seiring dengan peningkatan konektivitas dan pertukaran informasi secara daring, keamanan data dan pesan yang ditransmisikan melalui jaringan komunikasi menjadi semakin penting. Informasi dapat disampaikan melalui pesan yang dapat dibaca dan dimengerti maknanya dengan menggunakan berbagai bentuk seperti tulisan, gambar, ataupun simbol. Pesan dibagi menjadi beberapa macam, seperti pesan grup maupun pesan rahasia. Pesan rahasia adalah pesan yang hanya diketahui oleh individu yang berhak untuk menerimanya dan tidak dapat diambil oleh pihak lain. Pentingnya menjaga kerahasiaan pesan ini dapat dilihat dari fakta bahwa banyak pesan atau dokumen yang telah dikirim atau diterima telah mengalami perubahan oleh pihak yang tidak bertanggung jawab. Oleh sebab itu, diperlukan suatu prosedur yang dapat menjaga kerahasiaan pesan.

Untuk menjaga kerahasiaan dan integritas pesan yang dikirimkan adalah dengan menggunakan kriptografi. Kriptografi merupakan ilmu yang berkaitan tentang metode-metode untuk mengamankan pesan atau informasi penting, menjaga integritas, dan otentikasi informasi agar dapat dibaca oleh pihak yang berwenang dengan menggunakan kunci rahasia yang dimilikinya. Meskipun kriptografi ini telah digunakan sejak zaman dahulu, namun tantangan keamanan di dunia digital yang terus berkembang mendorong untuk terus meningkatkan dan

mengembangkan teknik kriptografi. Tahap utama dalam penggunaan teknik kriptografi adalah proses enkripsi dan dekripsi. Proses enkripsi adalah sebuah proses penyandian yang melakukan perubahan sebuah kode (pesan) dari yang bisa dimengerti (plainteks) menjadi sebuah kode yang tidak bisa dimengerti (cipherteks) (Ariska et al., 2018). Sedangkan proses dekripsi adalah proses untuk mengubah pesan yang telah diacak (cipherteks) kembali ke pesan asli (plainteks) agar dapat dibaca oleh penerima pesan tersebut. Kriptografi ini memiliki dua jenis, yaitu kriptografi simetris maupun kriptografi asimetris. Kriptografi simetris melibatkan penggunaan satu kunci yang sama untuk melakukan proses enkripsi dan dekripsi. sementara itu, kriptografi asimetris memanfaatkan kunci publik dan kunci rahasia untuk melakukan proses enkripsi dan dekripsi pesan.

Pentingnya menjaga kerahasiaan pesan ini tidak dapat diabaikan, karena hal ini diperlukan untuk melindungi dan memastikan keamanan informasi penting yang hendak disampaikan kepada pihak yang berwenang. Dalam ajaran Islam juga sudah dijelaskan terkait pentingnya menjaga amanah, yang terdapat pada 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 ﴿٥٨﴾

Artinya: “*Sesungguhnya Allah menyuruh kamu menyampaikan Amanah kepada pemiliknya. Apabila kamu menetapkan hukum di antara manusia, hendaklah kamu tetapkan secara adil. Sesungguhnya Allah memberi pengajaran paling baik kepadamu. Sesungguhnya Allah maha mendengar lagi maha melihat*” (Lajnah Pentashihan Mushaf Al-Qur’an, 2019a)

Pada ayat tersebut telah dijelaskan mengenai pentingnya menyampaikan amanah kepada yang berhak. Sehingga, Amanah dalam kriptografi dapat diartikan sebagai menjaga kerahasiaan pesan yang akan disampaikan kepada penerima pesan.

Munculnya teknologi pada saat ini yang semakin mengalami kemajuan

hingga adanya komputer kuantum yang menyebabkan banyaknya algoritma kunci publik seperti El-Gamal maupun RSA (*Rivest Shamir Adleman*) mulai tidak aman untuk digunakan karena adanya komputer tersebut yang dapat melakukan pembobolan pesan sehingga pesan tidak bersifat rahasia kembali. Pada tahun 1990-an, Shor mengusulkan algoritma yang dapat memecahkan masalah faktorisasi bilangan bulat dan logaritma diskrit dalam waktu polinomial pada komputer kuantum (Danner & Kreuzer, 2020). Sehingga, algoritma ini kemudian diperluas dan menghasilkan Kriptografi *Pasca-Quantum*. Kriptografi *Pasca-Quantum* merupakan upaya untuk mengembangkan sistem kriptografi yang mampu mencegah serangan yang dapat dilakukan oleh komputer kuantum. Salah satu contoh kriptografi *pasca-quantum* yaitu kriptosistem *Niederreiter*.

Kriptosistem *Niederreiter* merupakan varian dari kriptosistem *McEliece* yang menawarkan beberapa perbaikan pada proses enkripsi dan dekripsi dan membutuhkan ukuran kunci publik yang lebih kecil dari *McEliece* (Danner & Kreuzer, 2020). Kriptosistem *Niederreiter* ini salah satu kriptosistem kunci publik berbasis teori kode yang dikembangkan oleh Harald Niederreiter pada tahun 1986, dimana kriptosistem *Niederreiter* telah memanfaatkan prinsip-prinsip aljabar linier dan teori kode untuk mengamankan pertukaran informasi. Sistem ini menggunakan matriks *parity check* dari sebuah kode linier sebagai dasar kriptografi. Kriptosistem ini menggunakan sindrom sebagai cipherteks. Enkripsi dari *Niederreiter* lebih cepat dibandingkan dengan enkripsi *McEliece*. Kelebihan yang diperoleh apabila menggunakan sistem ini yaitu tingkat keamanan yang tinggi terhadap serangan oleh komputer kuantum dan memiliki efisiensi yang baik dalam hal kecepatan enkripsi dan dekripsi. Kriptosistem ini memiliki kunci publik hingga 1MB untuk keamanan

klasik sekitar 256-bit (sesuai dengan keamanan pasca-kuantum 128-bit yang berarti bahwa sebuah komputer kuantum perlu melakukan setidaknya 2^{128} operasi yang menggunakan serangan paling terkenal) dengan menggunakan parameter kode Goppa biner (Wang et al., 2018). Oleh karena itu, kriptosistem *Niederreiter* dengan basis matematisnya yang kuat, dianggap mampu untuk menyediakan keamanan yang kuat di era *pasca quantum*.

Pilihan kode kesalahan yang baik digunakan untuk kriptosistem *Niederreiter* yaitu kode Goppa biner. Kode Goppa biner adalah kode koreksi kesalahan yang termasuk kelas kode Goppa umum yang mulanya telah dikenalkan oleh Valerii Denisovich Goppa pada tahun 1970-an, tetapi struktur binernya memberikan beberapa kelebihan dibandingkan dengan yang non biner. Dalam kriptografi, kode ini digunakan untuk menemukan support dan polinomial Goppa yang lebih besar. Polinomial Goppa adalah polinomial dengan koefisien biner yang memungkinkan deteksi dan koreksi kesalahan dengan efisien. Kelebihan dari menggunakan kode ini yaitu kemampuannya untuk mendeteksi dan memperbaiki kesalahan dalam transmisi data dengan tingkat keandalan yang tinggi (Ilmiyah, 2018). Kode Goppa biner sering digunakan dalam kriptografi *pasca-quantum* dimana keamanan data harus dijaga dari serangan oleh komputer kuantum. Dalam kriptografi, kode Goppa biner ini digunakan untuk melakukan pembentukan kunci pada kriptosistem *Niederreiter*.

Beberapa penelitian sebelumnya yang telah dilakukan adalah mengimplementasikan kriptosistem *Niederreiter* berbasis FPGA dengan menggunakan kode Goppa biner. Penelitian ini bertujuan untuk mengembangkan implementasi FPGA dari kriptosistem *Niederreiter* dengan menggunakan kode

Goppa biner. Untuk tahapan penelitiannya yaitu plaintexts dienkripsi dengan menggunakan kriptosistem *Niederreiter*. Kemudian dalam pembentukan kunci, parameter yang digunakan adalah dari kode Goppa biner. FPGA (*Field-Programmable Gate Array*) merupakan sebuah IC (*Integrated Circuit*) yang digunakan untuk mengimplementasikan rangkaian digital. Implementasi FPGA dapat disesuaikan dengan kinerja dan penggunaan sumber daya, baik untuk penggunaan sumber daya rendah dalam sistem tertanam atau kinerja tinggi sebagai akselerator untuk server (Danner & Kreuzer, 2020).

Peneliti ini dilakukan implementasi kode Goppa biner pada Kriptosistem *Niederreiter*. Dalam konteks kriptosistem *Niederreiter*, kode Goppa biner digunakan sebagai bagian dari proses enkripsi dan dekripsi untuk melindungi kerahasiaan dan integritas data. Implementasi kode Goppa biner pada Kriptosistem *Niederreiter* melibatkan proses pembentukan kunci, enkripsi, dan dekripsi. Kode Goppa biner digunakan untuk menghasilkan kunci publik dan kunci pribadi yang digunakan dalam proses enkripsi dan dekripsi oleh kriptosistem *Niederreiter*.

1.2 Rumusan Masalah

Berdasarkan latar belakang dari penelitian tersebut, maka rumusan masalah penelitian ini sebagai berikut:

1. Bagaimana proses simulasi pembentukan kunci kode Goppa biner pada Kriptosistem *Niederreiter*?
2. Bagaimanakah proses simulasi enkripsi pada pesan teks kriptosistem *Niederreiter* dengan menggunakan kode Goppa biner?
3. Bagaimanakah proses simulasi dekripsi pada pesan teks kriptosistem

Niederreiter dengan menggunakan kode Goppa biner?

1.3 Tujuan Penelitian

Berdasarkan pada rumusan masalah yang telah diuraikan sebelumnya, maka tujuan dari penelitian ini adalah sebagai berikut:

1. Menerapkan proses simulasi pembentukan kunci pada pesan teks dengan menggunakan kode Goppa biner.
2. Menerapkan proses simulasi enkripsi pada pesan teks menggunakan kriptosistem *Niederreiter* dengan kode Goppa biner.
3. Menerapkan proses simulasi dekripsi pada pesan teks menggunakan kriptosistem *Niederreiter* dengan kode Goppa biner.

1.4 Manfaat Penelitian

Ada beberapa manfaat yang dapat kita peroleh yaitu:

1. Mengimplementasikan kriptosistem *Niederreiter* pada pesan teks dengan menggunakan kode Goppa biner.
2. Menambah pengetahuan lebih dalam mengenai pengamanan pesan teks menggunakan kriptosistem *Niederreiter* dengan kode Goppa biner.
3. Memperbanyak bahan literasi dan informasi yang melingkupi kriptografi.

1.5 Batasan Masalah

Batasan masalah yang akan dijelaskan dalam penelitian ini adalah dengan menggunakan Tabel kode ASCII untuk mengkonversi bilangan biner.

1.6 Definisi Istilah

Berdasarkan rumusan masalah penelitian, maka uraian definisi istilah dalam penelitian ini adalah sebagai berikut:

1. Kode Goppa adalah kode linier koreksi kesalahan yang digunakan untuk proses enkripsi dan dekripsi pada kriptografi.
2. Kunci adalah suatu parameter yang digunakan untuk mengendalikan jalannya kriptografi.
3. Enkripsi merupakan proses mengubah atau mengkodekan pesan sehingga menjadi bentuk yang sulit dipahami atau dibaca oleh pihak yang tidak berwenang.
4. Dekripsi adalah proses untuk mengembalikan pesan yang telah dienkripsi ke bentuk semula.
5. ASCII (*American Standard Code for Information Interchange*) adalah suatu standar karakter dalam komputasi yang menetapkan representasi numerik untuk setiap huruf, angka, tanda baca, dan karakter khusus lainnya yang digunakan sebagai perubahan pesan asli menjadi sebuah urutan digit biner.

BAB II

KAJIAN TEORI

2.1 Teori Pendukung

2.1.1 Aritmatika Modulo

Definisi

Misalkan a adalah bilangan bulat dan $m > 0$. Operasi $a \bmod m$ memberikan sisa jika a dibagi dengan m . Selain itu, $a \bmod m = r$ sedemikian hingga $a = mx + r$, dengan $0 \leq r < m$ (Sari, 2018).

Contoh

1. $18 \bmod 5 = 3$ $(18 = 5 \cdot 3 + 3)$
2. $28 \bmod 9 = 1$ $(28 = 9 \cdot 3 + 1)$
3. $35 \bmod 7 = 0$ $(35 = 7 \cdot 5 + 0)$

2.1.2 Kongruensi

Definisi

Apabila $x, y, r \in \mathbb{Z}$ dan $r \neq 0$, maka x kongruen dengan $y \bmod r$ jika dan hanya jika r membagi $(x - y)$. Dinotasikan sebagai $x \equiv y \pmod{r}$ jika dan hanya jika $r | x - y$. Jika $x \equiv y \pmod{r}$, maka terdapat bilangan bulat k sehingga $x = y + kr$ (Handayani & Yulina, 2020).

Dikatakan x tidak kongruen dengan $y \bmod r$ apabila r tidak membagi $x - y$. Dinotasikan sebagai $x \not\equiv y \pmod{r}$ jika $r \nmid x - y$.

Contoh

1. $15 \equiv 3 \pmod{4}$ memiliki arti yang sama dengan $15 = 3 + (3 \cdot 4)$
2. $72 \equiv 2 \pmod{5}$ memiliki arti yang sama dengan $72 = 2 + (14 \cdot 5)$

Teorema

Kongruensi modulo r memenuhi sifat-sifat sebagai berikut:

1. Refleksif

Jika $x \in \mathbb{Z}$, maka $x \equiv x \pmod{r}$.

2. Simetris

Jika $x, y \in \mathbb{Z}$ sedemikian hingga $x \equiv y \pmod{r}$ maka $y \equiv x \pmod{r}$.

3. Transitif

Jika $x, y, z \in \mathbb{Z}$ sedemikian hingga $x \equiv y \pmod{r}$ dan $y \equiv z \pmod{r}$, maka $x \equiv z \pmod{r}$ (Handayani & Yulina, 2020).

Bukti

1. Jika $r \neq 0$, maka $r|0$ atau $r|x - x$ berarti $x \equiv x \pmod{r}$
2. Jika $x \equiv y \pmod{r}$ maka $r|x - y$. Diperoleh dari definisi keterbagian bahwa terdapat bilangan bulat k sehingga $kr = x - y$ atau $(-k)r = y - x$.

Sehingga $y \equiv x \pmod{r}$

3. Jika $x \equiv y \pmod{r}$ dan $y \equiv z \pmod{r}$ maka $r|x - y$ dan $r|y - z$. Terdapat bilangan bulat k dan t sehingga $kr = x - y$ dan $tr = y - z$.
Sehingga $r|x - z$ yaitu $x \equiv z \pmod{r}$.

Teorema

Misalkan $r \in \mathbb{Z}$. Jika $x \equiv y \pmod{r}$ dan a adalah sembarang bilangan bulat, maka

1. $(x + a) \equiv (y + a) \pmod{r}$
2. $xa \equiv ya \pmod{r}$

Bukti

Diketahui $x \equiv y \pmod{r}$ maka $r|x - y$

1. $x - y = x - y + a - a = (x + a) - (y + a)$

Maka $r|(x + a) - (y + a)$

Sehingga $(x + a) \equiv (y + a) \pmod{r}$

2. Terdapat bilangan bulat k ,

Maka $r|k(x - y) = r|kx - ky = r|kx - yk$

Sehingga $xk \equiv yk \pmod{r}$

Contoh

1. $37 \equiv 2 \pmod{7}$ maka $37 + 3 \equiv 2 + 3 \pmod{7}$ atau $40 \equiv 5 \pmod{7}$

2. $37 \equiv 2 \pmod{7}$ maka $37 \cdot 3 \equiv 2 \cdot 3 \pmod{7}$ atau $111 \equiv 6 \pmod{7}$

2.1.3 Kode Linear

Kode linear merupakan sebuah kode dari ruang vektor atas field berhingga yang berguna dalam pengkodean dan koreksi kesalahan. Kode linear yang digunakan dalam kriptosistem *Niederreiter* adalah kode Goppa.

Definisi (Kode Linear)

Suatu kode linear C dengan panjang n atas F_q adalah subruang dari ruang vektor F_q^n jika memenuhi (ling & xing, 2004):

1. $u + v \in V$;
2. $(u + v) + w = u + (v + w)$;
3. Terdapat elemen $0 \in V$ dengan sifat $0 + v = v = v + 0$ untuk semua $v \in V$;
4. Untuk setiap $u \in V$ terdapat elemen dari V , disebut $-u$, sedemikian hingga $u + (-u) = 0 = (-u) + u$;

5. $u + v = v + u$;
6. $\lambda v \in V$;
7. $\lambda(u + v) = \lambda u + \lambda v$;
8. Jika 1 adalah identitas perkalian dari F_q , maka $1u = u \forall u \in F_q$

Contoh

Diberikan ruang vector F_2^4 dan $C = \{0000, 0101, 1010, 1111\}$. Maka C merupakan kode linear.

Tabel 2.1 Operasi Penjumlahan

| | | | | |
|------|------|------|------|------|
| + | 0000 | 0101 | 1010 | 1111 |
| 0000 | 0000 | 0101 | 1010 | 1111 |
| 0101 | 0101 | 0000 | 1111 | 1010 |
| 1010 | 1010 | 1111 | 0000 | 0101 |
| 1111 | 1111 | 1010 | 0101 | 0000 |

Berdasarkan Tabel 2.1 dapat dilihat bahwa C memenuhi subruang, yaitu untuk setiap $u, v \in C, u + v \in C$.

Sehingga terbukti bahwa C merupakan kode linear.

Definisi

Misalkan V merupakan ruang vektor F_q dan $S = \{v_1, v_2, \dots, v_n\}$ adalah himpunan bagian tak kosong dari V . Maka dapat didefinisikan sebagai $\langle S \rangle = \{\lambda_1 v_1 + \dots + \lambda_n v_n : \lambda_i \in F_q, v_i \in S\}$.

Catatan

Jika S sudah menjadi subruang dari V , maka $\langle S \rangle = S$.

Contoh

Jika $q = 2$, dan $S = \{10101, 01010, 11001\}$, maka

$$\langle S \rangle = \{\lambda_1(10101) + \lambda_2(01010) + \lambda_3(11001) \mid \lambda_1, \lambda_2, \lambda_3 \in F_2\}$$

Tabel 2.2 Operasi Kode Linear

| λ_1 | λ_2 | λ_3 | $\lambda_1(10101) + \lambda_2(01010) + \lambda_3(11001)$ |
|-------------|-------------|-------------|--|
| 0 | 0 | 0 | 00000 |
| 0 | 0 | 1 | 11001 |
| 0 | 1 | 0 | 01010 |
| 0 | 1 | 1 | 01010+11001=10011 |
| 1 | 0 | 0 | 10101 |
| 1 | 0 | 1 | 10101+11001=01100 |
| 1 | 1 | 0 | 10101+01010=11111 |
| 1 | 1 | 1 | 10101+01010+11001=00110 |

Jadi ada 8 kombinasi yang diambil dari 2^3

Definisi (Kode Dual)

Diberikan kode linear C dengan panjang n atas F_q . Kode dual dari C , dinotasikan C^\perp adalah komplemen orthogonal dari C terhadap F_q^n . Misalkan $v = (v_1, v_2, \dots, v_n), w = (w_1, w_2, \dots, w_n) \in F_q^n$, maka:

1. Perkalian skalar dari v dan w adalah sebagai berikut:

$$v \cdot w = v_1w_1 + v_2w_2 + \dots + v_nw_n \in F_q$$

2. Vektor v dan w dikatakan orthogonal jika $v \cdot w = 0$

Contoh

Misalkan $F_q^n = F_2^5$ dan $C = \langle (10101), (01010), (11001) \rangle \in F_2^5$

Kode dual C^\perp adalah himpunan semua vector $w \in F_2^5$ yang orthogonal terhadap setiap elemen $v \in C$. Maka

$$C = \{w \in F_2^5 : (10101) \cdot w = 0 \wedge (01010) \cdot w = 0 \wedge (11001) \cdot w = 0\}$$

Misal $w = (w_1, w_2, w_3, w_4, w_5)$

$$(10101) \cdot w = 0 \Leftrightarrow w_1 + w_3 + w_5 = 0 \dots (1)$$

$$(01010) \cdot w = 0 \Leftrightarrow w_2 + w_4 = 0 \dots (2)$$

$$(11001) \cdot w = 0 \Leftrightarrow w_1 + w_2 + w_5 = 0 \dots (3)$$

Eliminasi (1) dan (3)

$$w_1 + w_3 + w_5 = 0$$

$$w_1 + w_2 + w_5 = 0$$

$$w_3 - w_2 = 0$$

$$w_3 = w_2$$

Eliminasi (2)

$$w_2 + w_4 = 0$$

$$w_4 = -w_2$$

$$w_4 = w_2$$

Eliminasi (3)

$$w_1 + w_2 + w_5 = 0$$

$$w_5 = -w_1 - w_2$$

$$w_5 = w_1 + w_2$$

Tabel 2.3 Nilai Vektor dari w

| w_1 | w_2 | w_3 | w_4 | w_5 |
|-------|-------|-------|-------|-------|
| 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 1 |
| 1 | 1 | 1 | 1 | 0 |

$$\begin{aligned} C^\perp &= \{w \in F_2^5 : (10101) \cdot w = 0 \wedge (01010) \cdot w = 0 \wedge (11001) \cdot w = 0\} \\ &= \{(00000), (01111), (10001), (11110)\} \end{aligned}$$

2.1.4 Kode Goppa

Kode Goppa biner merupakan salah satu jenis kode koreksi kesalahan yang digunakan dalam bidang teori kode. Kode ini ditemukan oleh matematikawan Brasil yang Bernama Valery Denisovich Goppa pada tahun 1970 (Singh, 2019). Kode Goppa memiliki parameter $[n, k, d]$. Pada kode

Goppa diberikan:

1. Sebuah polinomial berderajat t terdapat $g(x) \in GF(p^m)[x]$, dan
2. Sebuah himpunan n elemen dari $GF(p^m)$, $\{\alpha_0, \alpha_1, \dots, \alpha_{n-1}\}$, yang bukan nol dari $g(x)$.

Adapun sifat-sifat dari kode tersebut antara lain:

1. Panjang dari *codeword* $n \leq 2^m$
2. Jarak kode $d \geq 2t + 1$
3. $k \geq n - mt$ simbol informasi

Definisi

Misalkan $g(x) = g_0 + g_1x + g_2x^2 + \dots + g_tx^t \in GF(p^m)[x]$, dan $L = \{\alpha_1, \alpha_2, \dots, \alpha_n\} \subseteq GF(p^m)$, sedemikian hingga $g(\alpha_i) \neq 0$, untuk semua $\alpha_i \in L$ dan Untuk setiap i (di mana $1 \leq i \leq n$), Sehingga dapat didefinisikan sebagai

$$\left\{ c = (c_1, c_2, \dots, c_n) \in GF(p^m) : \sum_{i=1}^n \frac{c_i}{x - \alpha_i} \equiv 0 \pmod{g(x)} \right\}$$

dapat disebut kode Goppa dengan parameter $g(x)$ dan L yang dapat dinotasikan sebagai $\Gamma(L, g(x))$. (Singh, 2020).

Teorema

Perhatikan bahwa

$$(x - \alpha_i) \left(-\frac{g(x) - g(\alpha_i)}{z - \alpha_i} g(\alpha_i)^{-1} \right) \equiv 1 \pmod{g(x)},$$

Dan $\frac{g(x) - g(\alpha_i)}{z - \alpha_i}$ adalah sebuah polinomial, maka modulo $g(x)$, $1/(x - \alpha_i)$ dapat

dianggap sebagai polinomial juga, yaitu:

$$\frac{1}{x - \alpha_i} \equiv -\frac{g(x) - g(\alpha_i)}{z - \alpha_i} g(\alpha_i)^{-1} \pmod{g(x)}.$$

Oleh sebab itu, kekongruenan dari $R_c(x) \equiv 0 \pmod{g(x)}$ didefinisikan sebagai $\Gamma(L, g)$ yang berarti $g(x)$ membagi polinomial.

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

Tetapi, perhatikan bahwa $\frac{g(x) - g(\alpha_i)}{z - \alpha_i}$ adalah polinomial berderajat $< t$ jika

$g(x)$ berderajat t , sehingga $c \in \Gamma(L, g)$ jika dan hanya jika

$$\sum_{i=1}^n c_i \frac{g(x) - g(\alpha_i)}{z - \alpha_i} g(\alpha_i)^{-1} = 0$$

adalah sebuah polinomial.

Diperoleh dari definisi bahwa kode Goppa adalah linear (Ling & Xing, 2004).

Akibat

Untuk sebuah polinomial Goppa $g(x)$ berderajat t dan $L = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$,

didapatkan $H = CXY$ untuk

$$C = \begin{bmatrix} -g_t & -g_{t-1} & -g_{t-2} & \dots & -g_1 \\ 0 & -g_t & -g_{t-1} & \dots & -g_2 \\ 0 & 0 & -g_t & \dots & -g_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & -g_t \end{bmatrix}, X = \begin{bmatrix} \alpha_1^{t-1} & \alpha_2^{t-1} & \dots & \alpha_n^{t-1} \\ \alpha_1^{t-2} & \alpha_2^{t-2} & \dots & \alpha_n^{t-2} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ 1 & 1 & \dots & 1 \end{bmatrix},$$

$$Y = \begin{bmatrix} h_1 & 0 & 0 & \dots & 0 \\ 0 & h_2 & 0 & \dots & 0 \\ 0 & 0 & h_3 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & h_n \end{bmatrix}$$

Karena C invertible, matriks parity check H lain dari kode tersebut adalah

$$H' = XY = \begin{bmatrix} \alpha_1^{t-1} h_1 & \alpha_2^{t-1} h_2 & \dots & \alpha_n^{t-1} h_n \\ \alpha_1^{t-2} h_1 & \alpha_2^{t-2} h_2 & \dots & \alpha_n^{t-2} h_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1 h_1 & \alpha_2 h_2 & \dots & \alpha_n h_n \\ h_1 & h_2 & \dots & h_n \end{bmatrix}$$

Terdapat $c \in \Gamma(L, g)$ jika dan hanya jika $cH^T = 0$, yang mengimplikasikan

$c(CXY)^T = 0$, secara ekuivalen $cY^T X^T C^T = 0$, menghasilkan $cY^T X^T = 0$ atau $c(XY)^T = 0$

Catatan

Elemen dari $GF(p^m)$ sebagai vektor dengan Panjang m dengan ruang vektor isomorfisme dan memiliki matriks *parity check* H untuk $\Gamma(L, g)$ dari $GF(p^m)$ sebagai matriks $mt \times n$, dengan t kolom yang independen secara linear dari $GF(p^m)$. Sehingga, diketahui jarak kode Goppa $d(\Gamma(L, g)) \geq 2t + 1$ dan dimensi dari kode Goppa yaitu $k(\Gamma(L, g)) \geq n - mt$ (Singh, 2020).

Definisi (Polinomial Primitif)

Polinomial primitif merupakan sebuah polinomial yang memiliki koefisien yang saling prima relatif. Polinomial ini disebut primitif jika terdapat bilangan bulat positif n sedemikian hingga setiap koefisien dalam $f(x)$ adalah kelipatan dari n , dan n bilangan bulat positif terkecil. Contohnya, $f(x) = x^3 + x^2 + 1$ adalah sebuah polinomial primitif yang berderajat 3 oleh lapangan biner F_2 .

2.1.5 Encoding Kode Goppa

Misalkan $\Gamma(L, g(z))$ sebuah kode Goppa, dimana $g(z)$ suatu polinomial primitif dengan $\deg(g(z)) = t$ dan $|L| = n$. Misalkan $\mathbb{F}_q(\Gamma(L, g(z))) = k$ dan matriks *parity-check* H berukuran $(n - k) \times n$ untuk masing-masing kode Goppa. Maka, proses *encoding* kode Goppa menggunakan pesan dengan panjang n -bit oleh \mathbb{F}_q adalah mH (Singh, 2020).

2.1.6 Decoding Kode Goppa

Misal vektor $y = (y_1, y_2, \dots, y_n)$ kata kode yang diterima dan memuat r buah eror, di mana $2r + 1 \leq d$ (Singh, 2020). Proses untuk mencari *decoding* kode Goppa, sebagai berikut:

1. Temukan z menggunakan $HZ^T = S^{-1}c$;
2. Hitung sindrom

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

3. Selesaikan persamaan kunci

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

4. Tentukan himpunan lokasi eror $B = \{i | \sigma(\alpha_i) = 0\}$
5. Masukkan hasil yang diperoleh untuk mendapatkan pesan asli

$$m = m' \cdot p$$

2.1.7 Finite Field (Lapangan Hingga)

Definisi

Sebuah himpunan tak kosong F dari elemen-elemen dengan dua operasi $+$ (disebut penjumlahan) dan \cdot (disebut perkalian) yang memenuhi aksioma-aksioma untuk semua $a, b, c \in F$:

1. F tertutup di bawah $+$ dan $-$, yaitu $a + b$ dan $a - b$ ada di dalam F ;
2. Komutatif: $a + b = b + a, a - b = b - a$;
3. Asosiatif: $(a + b) + c = a + (b + c), a - (b - c) = (a - b) - c$;
4. Distributif: $(a - (b + c)) = a - b + a - c$.

Dua elemen identitas yang berbeda 0 dan 1 (disebut aditif dan identitas

multiplikatif) yang memenuhi hal berikut:

1. $a + 0 = a$ untuk semua $a \in F$;
2. $a \cdot 1 = a$ dan $a \cdot 0 = 0$ untuk semua $a \in F$;
3. Untuk setiap a di F , ada elemen invers aditif $(-a)$ di F sehingga $a + (-a) = 0$;
4. Untuk setiap $a \neq 0$ di F , terdapat sebuah elemen invers multiplikatif a^{-1} di F sehingga $a \cdot a^{-1} = 1$ (ling & xing, 2004).

Lemma

Misalkan a, b adalah sebarang dua elemen dari sebuah F . Maka

1. $(-1) \cdot a = -a$;
2. $ab = 0$ mengimplikasikan $a = 0$ atau $b = 0$.

Contoh

1. Himpunan semua bilangan bulat $\mathbf{Z} := \{0, \pm 1, \pm 2, \dots\}$ membentuk sebuah ring di bawah penjumlahan dan perkalian. Hal ini disebut ring bilangan bulat.
2. Himpunan semua polynomial di atas bidang F , $F[x] := \{\alpha_0 + \alpha_1 x + \dots + \alpha_n x^n : \alpha_i \in F, n \geq 0\}$, membentuk sebuah ring penjumlahan dan perkalian polinomial.

Definisi

Misalkan a, b dan $m > 1$ bilangan bulat. Dikatakan bahwa a kongruen dengan $b \pmod m$, ditulis sebagai $a \equiv b \pmod m$, jika $m | (a - b)$ yaitu m membagi $a - b$.

Contoh

1. $47 \equiv 2(\text{mod } 5)$
2. $a \equiv 0(\text{mod } 2)$ berarti a genap
3. $a \equiv 1(\text{mod } 2)$ berarti a ganjil

Pernyataan

Diberikan bilangan bulat a dan $m > 1$, dengan algoritma pembagian menghasilkan $a = mq + b$, dimana b ditemukan oleh a dan m , dan $0 \leq b \leq m - 1$. Oleh karena itu, setiap bilangan bulat a kongruen dengan salah satu dari $0, 1, \dots, m - 1$ modulo m . Jika $a \equiv b(\text{mod } m)$ dan $c \equiv d(\text{mod } m)$, maka kita memiliki

$$a + c \equiv b + d(\text{mod } m),$$

$$a - c \equiv b - d(\text{mod } m),$$

$$a \times c \equiv b \times d(\text{mod } m)$$

Untuk sebuah bilangan bulat $m > 1$, kita nyatakan dengan Z_m himpunan $\{0, 1, \dots, m - 1\}$ dan didefinisikan penjumlahan dan perkalian dalam Z_m dengan:

$$a + b = \text{sisa dari } a + b \text{ dibagi dengan } m, \text{ yaitu } (a + b(\text{mod } m)),$$

$$a \cdot b = \text{sisa dari } ab \text{ dibagi dengan } m, \text{ yaitu } (ab(\text{mod } m)).$$

Oleh karena itu, Z_m dengan penjumlahan dan perkalian yang telah didefinisikan sehingga membentuk sebuah ring. Z_m merupakan *field* jika dan hanya jika m bilangan prima (Ling & Xing, 2004).

Definisi (Ring Polinomial)

Misalkan F *field*. Terdapat himpunan

$$F[x] := \left\{ \sum_{i=0}^n \alpha_i x^i : \alpha_i \in F, n \geq 0 \right\}$$

disebut ring polinomial dari F . Sebuah elemen dari $F[x]$ disebut polinomial dari

F . Untuk polinomial $F[x] = \sum_{i=0}^n \alpha_i x^i$, bilangan bulat n disebut berderajat $f(x)$, yang dinotasikan dengan $\deg(f(x))$, jika $\alpha_n \neq 0$. Sebuah polinomial tak nol berderajat n jika $\alpha_n = 1$. Polinomial $f(x)$ berderajat positif disebut dapat direduksi jika ada dua polinomial $g(x)$ dan $h(x)$ dari F sedemikian hingga $\deg(g(x)) < \deg(h(x)) < \deg(f(x))$ dan $f(x) = g(x)h(x)$. Begitupun sebaliknya, jika tidak $f(x)$ berderajat positif maka dikatakan tidak dapat direduksi (Ling & Xing, 2004).

Contoh

1. Polinomial $f(x) = x^4 + 2x^6 \in \mathbf{Z}_3[x]$ berderajat 6. Polinomial ini dapat direduksi sebagai $f(x) = x^4(1 + 2x^2)$.
2. Polinomial $g(x) = 1 + x + x^2 \in \mathbf{Z}_2[x]$ berderajat 2 dikatakan tidak dapat direduksi karena polinomial tersebut tidak memiliki faktor linier.

Teorema

Misalkan $f(x)$ merupakan polinomial atas sebuah F Field dengan berderajat \geq

1. Maka ring $F[x]/\langle f(x) \rangle$ adalah suatu bidang jika dan hanya jika $f(x)$ adalah polinomial tak tereduksi pada F (Singh, 2019).

Contoh

Ring $\mathbf{Z}_2[x]/\langle 1 + x + x^2 \rangle = \{0, 1, x, 1 + x\}$ adalah sebuah bidang yang berorde $2^2 = 4$.

Secara umum, untuk polinomial tak tereduksi berderajat k , $f(x) \in F[x]$, dimana $|F| = p$, $F[x]/\langle f(x) \rangle$ adalah orde p^k . Sebuah *finite field* dari orde q , yang dinotasikan oleh F_q , dimana $q = p^n$ untuk suatu bilangan prima p dan bilangan asli n sebagai berikut:

$$F_q = \frac{\mathbb{Z}_p[x]}{\langle f(x) \rangle}$$

$$= \{\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \dots + \alpha_{n-1} x^{n-1} + \langle f(x) \rangle\}$$

untuk $i \in \{0, 1, \dots, n-1\}, \alpha_i \in \mathbb{Z}_p$

dimana $\mathbb{Z}_p[x]$ adalah polinomial ring dengan variabel x dan koefisien dari \mathbb{Z}_p dan $f(x)$ adalah polinomial tak tereduksi berderajat n dari \mathbb{Z}_p .

Definisi (Elemen Primitif)

Sebuah elemen α dalam sebuah *finite field* F_q dikatakan elemen primitif dari F_q jika $F_q = \{0, \alpha, \alpha^2, \dots, \alpha^{q-1}\}$ (Ling & Xing, 2004).

Contoh

Finite field $F_4 = F_2[\alpha]$, di mana α adalah akar dari polinomial tak tereduksi $\alpha^2 + \alpha + 1 \in F_2[x]$. Maka

$$\alpha^2 = -(1 + \alpha) = 1 + \alpha, \alpha^3 = \alpha(\alpha^2) = \alpha(1 + \alpha) = \alpha + \alpha^2 = \alpha + 1 + \alpha = 1.$$

Dengan demikian, $F_4 = \{0, \alpha, 1 + \alpha, 1\} = \{0, \alpha, \alpha^2, \alpha^3\}$, jadi α elemen primitif.

Definisi (*Galois Field*)

Sebuah elemen *Galois Field* (GF) terdiri dari sekumpulan elemen primitif yang dinotasikan oleh α dan bernilai $0, \alpha^0, \alpha^1, \alpha^2, \dots, \alpha^{n-1}$. *Galois Field* digunakan dalam bentuk $GF(p^m)$, dengan p adalah bilangan prima dari *Galois Field* dan $m \in \mathbb{Z}$ sebagai eksponen. Untuk membentuk sebuah himpunan dari elemen 2^m , dimana $n = 2^m - 1$. *Galois field* ini dengan $GF(2^m)$.

Operasi penjumlahan dan perkalian pada $GF(2^m)$ mirip dengan penjumlahan polinomial biasa, yang membedakan hanya pada koefisien yang terjadi pada $GF(2^n)$ yang menggunakan penjumlahan dan perkalian 2 elemen dengan modulo 2 seperti pada Tabel 2.4.

Tabel 2. 4 Operasi Penjumlahan dan Perkalian $GF(2^4)$

| | | |
|---|---|---|
| + | 0 | 1 |
| 0 | 0 | 1 |
| 1 | 1 | 0 |

| | | |
|---|---|---|
| − | 0 | 1 |
| 0 | 0 | 1 |
| 1 | 1 | 0 |

| | | |
|---|---|---|
| × | 0 | 1 |
| 0 | 0 | 0 |
| 1 | 0 | 1 |

Pembentukan Galois Field (GF)

Galois Field (GF) memiliki dua elemen didalamnya, yaitu 0 dan 1.

Sebagai contoh, jika $GF(2^3)$ dengan polinomial $f(x) = x^3 + x^2 + 1$, maka $2^3 = 8$ elemen yaitu $\{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$. Sehingga diperoleh nilai elemen untuk $GF(2^3)$ sebagai berikut:

Tabel 2.5 Elemen dari $GF(2^3)$

| Index | Polinomial | Biner |
|------------|-------------------------|-------|
| 0 | 0 | 000 |
| α^0 | 1 | 100 |
| α^1 | α | 010 |
| α^2 | α^2 | 001 |
| α^3 | $1 + \alpha^2$ | 101 |
| α^4 | $1 + \alpha + \alpha^2$ | 111 |
| α^5 | $1 + \alpha$ | 110 |
| α^6 | $\alpha + \alpha^2$ | 011 |

2.1.8 Kriptografi

Kriptografi berasal dari Bahasa Yunani, yakni “*kryptos*” dan “*graphia*”.

“*kryptos*” memiliki arti yaitu sesuatu yang disembunyikan, bersifat rahasia dan

tidak dikenal. Sedangkan arti dari “*graphia*” adalah tulisan. Sehingga secara definisi, kriptografi adalah tulisan yang disembunyikan atau bersifat rahasia.

Kriptografi merupakan ilmu matematika yang berkaitan dengan metode pengamanan informasi, termasuk komunikasi dan penyimpanan data agar hanya pihak yang berhak atau yang memiliki kunci sesuai yang dapat membaca informasi tersebut. Aspek-aspek dalam kriptografi adalah sebagai berikut:

1. Kerahasiaan (*confidentiality*), yaitu untuk menjaga isi dari informasi dari pihak yang tidak berwenang untuk mendapatkannya.
2. Integritas data (*data integrity*), yaitu menjamin bahwa pesan yang dikirim masih asli dan tidak dimanipulasi.
3. Otentikasi (*authentication*), yaitu berhubungan dengan identifikasi, seperti mengidentifikasi suatu kebenaran pihak antara pengirim dan penerima pesan.
4. Anti-penyangkalan, yaitu untuk mencegah pihak yang saling berkomunikasi melakukan penyangkalan.

Terdapat beberapa istilah dalam kriptografi yang penting untuk diketahui, sebagai berikut:

1. Pengirim pesan, yaitu orang yang mengirimkan pesan kepada seorang penerima.
2. Penerima pesan, yaitu orang yang mendapatkan pesan yang dikirim oleh pengirim pesan.
3. Pesan, yaitu informasi atau data yang dapat dipahami maknanya.
4. Plainteks, yaitu pesan asli yang masih belum tersandi.
5. Cipherteks, yaitu pesan yang telah disandikan ke bentuk lain sehingga

tidak bisa dibaca oleh orang lain, kecuali orang tersebut mengetahui kuncinya.

6. Kunci, yaitu parameter yang digunakan dalam proses enkripsi dan dekripsi.
7. Enkripsi, yaitu proses menyandikan plainteks menjadi cipherteks.
8. Dekripsi, yaitu proses mengubah cipherteks menjadi plainteks.
9. Kriptanalisis, yaitu ilmu untuk memecahkan cipherteks menjadi plainteks tanpa diketahui kuncinya.

Algoritma kriptografi dibagi menjadi dua macam, yaitu:

1. Algoritma kunci publik

Algoritma kunci publik adalah algoritma kriptografi yang menggunakan dua buah kunci berbeda untuk proses enkripsi dan dekripsi. Kunci publik yang digunakan untuk proses enkripsi dan kunci rahasia digunakan untuk proses dekripsi.

2. Algoritma kunci rahasia

Algoritma kunci rahasia melibatkan satu kunci yang sama untuk proses enkripsi dan dekripsi. Salah satu kelemahan yang dimiliki oleh algoritma ini terletak pada sulitnya menjaga kesinkronan kunci privat (Ilmiah, 2018).

Terdapat banyak metode kriptografi yang dapat diterapkan, tetapi dalam klasifikasi secara umum terdiri dari dua metode, sebagai berikut:

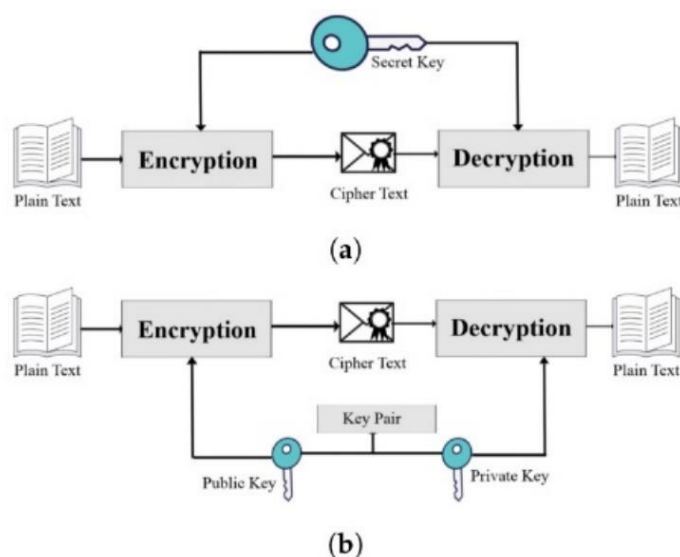
1. Kriptografi Simetris

Proses enkripsi dan dekripsi pada kriptografi simetris hanya menggunakan satu kunci. Sehingga, kunci ini harus dijaga kerahasiaannya dan diberikan

kepada pengirim dan penerima yang berwenang untuk melakukannya.

2. Kriptografi Asimetris

Proses enkripsi dan dekripsi pada kriptografi asimetris menggunakan pasangan kunci, yaitu kunci publik yang akan digunakan oleh pengirim untuk enkripsi dan kunci privat yang akan digunakan penerima untuk melakukan dekripsi yang hanya diketahui oleh mereka (Farooq et al., 2023).



Gambar 2.1 (a) Kriptografi Simetris (b) Kriptografi Asimetris.

Dalam kriptografi modern, pesan semula dikonversi menjadi bentuk biner yaitu 0 dan 1. Kriptografi ini juga bisa menggunakan ASCII untuk proses enkripsi yaitu dengan mengubah plaintext menjadi bentuk biner.

Kriptosistem merupakan sistem komputer yang didalamnya melibatkan kriptografi. Kriptosistem ini memuat tiga algoritma yang digunakan untuk mengamankan pesan, yaitu algoritma pembentukan kunci, algoritma enkripsi, dan algoritma dekripsi (Ilmiah, 2018). Kriptosistem dikembangkan dari

kriptografi yang sederhana dengan menambahkan sifat – sifat keamanan yang lebih tinggi, sehingga dapat digunakan untuk mengembangkan protokol kriptografi yang lebih kompleks dan aman, seperti digunakan dalam komunikasi rahasia dan pengamanan data.

2.1.9 Kriptosistem *Niederreiter*

Kriptosistem *Niederreiter* dipublikasikan pada tahun 1978 oleh Harald Niederreiter. Kriptosistem *Niederreiter* adalah salah satu jenis kriptosistem asimetris yang menggunakan teori kode pada dasarnya. Kriptosistem ini merupakan pengembangan dari kriptosistem *McEliece* yang menggunakan sebuah matrik *parity check H* untuk enkripsi (Wang et al., 2018). Kriptosistem *Niederreiter* hanya membutuhkan kunci yang lebih pendek. Bahkan, kriptosistem ini memungkinkan untuk menggunakan kunci publik hanya $S \cdot H \cdot P$ (Baldi, 2014)

Dalam menentukan kriptosistem *Niederreiter*, ada tiga langkah yang harus dilakukan yaitu pembentukan kunci, proses enkripsi, dan proses dekripsi. Ukuran n, k, d adalah parameter dari sistem publik, tetapi untuk g, P, S adalah kunci rahasia yang dihasilkan secara acak (Singh, 2019). Matriks *parity check H* adalah elemen-elemen dari $GF(2^m)$. Kode yang akan digunakan ada kode Goppa biner dengan sifat-sifat berikut:

1. Panjang kode $n \leq q + 1$;
2. Dimensi kode $k = n - mt$;
3. Jarak $d = 2t + 1$.

Proses pembentukan kunci

Proses pembentukan kunci dilakukan oleh penerima pesan dengan menggunakan sebuah kode yang akan dipilih. Proses ini akan menghasilkan pasangan kunci publik dan kunci privat berdasarkan nilai yang tersedia. Untuk langkah-langkahnya yaitu:

1. Memilih matriks permutasi P dengan ukuran $n \times n$;
2. Memilih matriks S *non-singular* dengan ukuran $(n - k) \times (n - k)$;
3. Hitung matriks *parity check* H dengan ukuran $(n - k) \times n$;
4. Kunci publik: matriks $S \cdot H \cdot P$ dengan ukuran $(n - k) \times n$;
5. Kunci rahasia: matriks S, H, P .

Proses enkripsi

Proses enkripsi dilakukan oleh pengirim pesan yang akan dikirimkan ke penerima pesan, dengan menggunakan langkah-langkah sebagai berikut:

1. Pengirim memiliki suatu pesan m dengan Panjang n -bit dengan berat $t \leq r/2$.
2. Hitung kemudian kirimkan cipherteks $c = S \cdot H \cdot P \cdot m^T$

Proses dekripsi

Proses dekripsi dilakukan oleh penerima pesan untuk memperoleh pesan asli, dengan langkah berikut:

1. Menemukan z sedemikian hingga $H z^T = S^{-1} c$;
2. Dengan menggunakan algoritma *decoding* untuk memecahkan vektor z yang digunakan dalam memperoleh $z - m \cdot P^T$, vektor kesalahan $m \cdot P^T$, dengan demikian, pesan m telah didapatkan.

2.2 Kajian Integrasi Topik Dengan Al-Qur'an

Al-Qur'an merupakan kitab suci Islam yang diwahyukan Allah SWT kepada

Nabi Muhammad SAW. sebagai rahmat dan petunjuk bagi manusia. Al-Qur'an mengandung banyak ilmu didalamnya termasuk ilmu pengetahuan yang menjelaskan segala sesuatu. Ilmu pengetahuan yang disampaikan dalam Al-Qur'an bisa berbentuk tersirat maupun tersurat.

Dalam ayat Al-Qur'an dijelaskan bahwa Allah SWT memerintahkan kepada umat manusia untuk menyampaikan pesan atau amanah hanya kepada orang yang berhak untuk menerimanya saja. Amanah merupakan segala sesuatu yang dipertanggungjawabkan kepada Allah SWT baik berupa perkataan maupun perbuatan. Allah SWT telah berfirman dalam Al-Qur'an surah Al-Ahzab ayat 72:

إِنَّا عَرَضْنَا الْأَمَانَةَ عَلَى السَّمَوَاتِ وَالْأَرْضِ وَالْجِبَالِ فَأَبَيْنَ أَنْ يَحْمِلْنَهَا وَأَشْفَقْنَ مِنْهَا وَحَمَلَهَا الْإِنْسَانُ
إِنَّهُ كَانَ ظَلُومًا جَهُولًا ﴿٧٢﴾

Artinya: “*Sesungguhnya Kami telah mengemukakan amanah kepada langit, bumi, dan gunung-gunung, maka semuanya enggan untuk memikul amanah itu dan mereka khawatir akan mengkhianatinya, dan dipikullah amanah itu oleh manusia. Sesungguhnya manusia itu amat zalim dan amat bodoh.*” (Lajnah Pentashihan Mushaf Al-Qur'an, 2019c).

Dalam tafsir Al-Wajiz, menjelaskan bahwa setelah meminta orang-orang beriman untuk menjaga ketakwaan, Allah SWT lalu menjelaskan bahwa salah satu wujud takwa adalah menjaga amanah. “Sesungguhnya Kami telah menawarkan amanat, yakni tugas-tugas keagamaan, kepada langit, bumi, dan gunung-gunung, tetapi semuanya enggan untuk memikul tanggung jawab amanat itu dan mereka khawatir tidak akan mampu melaksanakannya, lalu Kami menawarkan amanat itu kepada manusia, dan dipikullah amanat itu oleh manusia. Sungguh, manusia itu sangat zalim karena menyatakan sanggup memikul amanat tetapi secara sengaja menyalahkannya, dan sangat bodoh karena menerima amanat tetapi sering lengah dan lupa menjalankan atau memenuhinya” (Lajnah Pentashihan Mushaf Al-Qur'an, 2016).

Amanat dapat diartikan sebagai segala sesuatu yang diserahkan kepada seseorang untuk dipelihara dan ditunaikan dengan sebaik-baiknya serta berusaha maksimal untuk tidak menyiakannya. Apapun bentuk amanat, harus dipertanggungjawabkan oleh penerima kepada pemberi amanat.

Kriptografi adalah ilmu yang mempelajari tentang metode untuk menyamarkan pesan asli menjadi pesan rahasia sehingga pesan hanya dapat dibaca oleh penerima. Pesan rahasia dapat dianggap sebagai amanah yang harus dijaga kerahasiaannya hingga sampai ke penerima, seperti yang ada dalam Al-Qur'an surah Al-Anfal ayat 27, Allah SWT berfirman:

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

Artinya: “Wahai orang-orang beriman! Janganlah kamu mengkhianati Allah dan Rasul dan (juga) janganlah kamu mengkhianati amanah yang dipercayakan kepadamu, sedang kamu mengetahui” (Lajnah Pentashihan Mushaf Al-Qur'an, 2019a).

Berdasarkan (Al-Asyqor, 2007) menjelaskan bahwa Allah SWT melarang mereka untuk mengkhianati Rasulullah SAW dengan meninggalkan suatu kewajiban yang ditetapkan kepada mereka atau mengkhianati suatu amanat yang diberikan kepada mereka.

Surah ini menjelaskan bahwa adanya larangan untuk berkhianat dan kewajiban untuk amanah. Dalam konteks kriptografi, tujuan utamanya adalah untuk melindungi kerahasiaan, integritas, dan keaslian pesan atau informasi. Sehingga hal ini sejalan dengan prinsip-prinsip Islam yang mendorong umat muslim untuk menjaga amanah, termasuk menjaga kerahasiaan pesan atau informasi penting yang dipercayakan kepada mereka.

وَالَّذِينَ هُمْ لِأَمْتِهِمْ وَعَهْدِهِمْ رَاعُونَ ﴿٨﴾

Artinya: “dan orang-orang yang memelihara amanat dan janji mereka” (Q.S Al-Mu'minun:8) (Lajnah Pentashihan Mushaf Al-Qur'an, 2019b).

Menurut tafsir tahlili menjelaskan bahwa memelihara amanat-amanat yang dipikulnya dan menepati janjinya. Dalam ayat ini Allah SWT menerangkan sifat keenam dari orang mukmin yang beruntung itu adalah suka memelihara amanat-amanat yang dipikulnya, baik dari Allah SWT ataupun dari sesama manusia, yaitu bilamana kepada mereka dititipkan barang atau uang sebagai amanat yang harus disampaikan kepada orang lain, maka mereka benar-benar menyampaikan amanat itu sebagaimana mestinya, dan tidak berbuat khianat. Demikian pula bila mereka mengadakan perjanjian, mereka memenuhinya dengan sempurna. Mereka menjauhkan diri dari sifat kemunafikan seperti tersebut dalam sebuah hadis masyhur, yang menyatakan bahwa tanda-tanda orang munafik itu ada tiga, yaitu kalau berbicara suka berdusta, jika menjanjikan sesuatu suka menyalahi janji dan jika diberi amanat suka berkhianat (Cahaya, 2011)

Sumber utama dalam ajaran Islam yang membentuk dasar bagi keyakinan umat Islam selain Al-Qur'an juga terdapat hadis. Hadis merupakan perkataan, perbuatan, atau persetujuan yang diriwayatkan dari Nabi Muhammad SAW yang berfungsi untuk menjelaskan Al-Qur'an. Nabi Muhammad SAW memberikan petunjuk tentang menjaga amanah dalam berbagai aspek kehidupan. Amanah juga merupakan sifat dari nabi dan rasul dimana sifat tersebut yang selalu terjaga dan dijaga oleh Allah SWT. Sifat yang dimaksud adalah sifat wajib rasul, seperti berikut:

1. *Shiddiq*

Shiddiq berarti benar atau jujur. Yang dimaksud benar yaitu sifat Rasulullah SAW yang dapat dibenarkan baik dari perkataan maupun perbuatannya. Segala sesuatu yang datang dari Allah SWT kepada Rasulullah, baik itu

perintah, larangan, maupun keputusan pasti benar adanya karena rasul memiliki maksud untuk mewujudkan kebenaran yang telah diberikan oleh Allah SWT. Sifat *shiddiq* ini penting untuk diamalkan di berbagai aspek kehidupan. Seperti dalam hal bersosial, sifat ini baik digunakan untuk menyampaikan sebuah informasi sehingga informasi yang disampaikan tidak ada kebohongan pada isi pesan tersebut (Fajriyah et al., 2021).

2. Amanah

Amanah berarti dapat dipercaya. Dengan kata lain, amanah merupakan tanggung jawab yang telah dititipkan dalam menjalankan tugas dan kewajiban. Hal ini penting digunakan dalam penyampaian pesan yang harus dijaga kerahasiaannya, karena pesan yang telah diterima dapat dipercaya orisinalitasnya. (Fajriyah et al., 2021).

3. *Tabligh*

Tabligh berarti menyampaikan. Menyampaikan yang dimaksud adalah Nabi Muhammad SAW menyampaikan apa yang telah Allah SWT perintahkan kepada umat-Nya dengan tidak mengurangi perintah yang telah diterima (Musyirifin, 2020).

4. *Fathanah*

Fathanah memiliki arti cerdas atau pandai. Cerdas yang dimaksud tidak hanya kecerdasan intelektual saja, melainkan kecerdasan emosional dan kecerdasan spiritual juga dibutuhkan dalam sifat *fathanah* (Musyirifin, 2020).

Dalam kriptografi, amanah penting dilakukan karena itu merupakan salah satu yang terdapat pada sifat wajib Rasul, seperti dalam hadis Rasulullah SAW:

حَلَّنَا أَبُو بَكْرٍ بْنُ أَبِي شَيْبَةَ حَلَّنَا يَحْيَى بْنُ آدَمَ حَلَّنَا ابْنُ أَبِي ذَيْبٍ عَنْ عَبْدِ الرَّحْمَنِ بْنِ

عَطَاءٍ عَنْ عَبْدِ الْمَلِكِ بْنِ جَابِرٍ بْنِ عَتِيكَ عَنْ جَابِرِ بْنِ عَبْدِ اللَّهِ قَالَ رَسُولُ اللَّهِ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ إِذَا حَدَّثَ الرَّجُلُ حَدِيثًا ثُمَّ لَمَّتْ فَهِيَ أَمَانَةٌ (رواه أبو داود)

Artinya: “Telah menceritakan kepada kami [Abu Bakar bin Abu Syaibah] berkata, telah menceritakan kepada kami [Yahya bin Adam] berkata, telah menceritakan kepada kami [Ibnu Abu Dzi’b] dari [‘Abdurrahman bin Atha] dari [Abdul Malik bin Jabir bin Atik] dari [Jabir bin Abdullah] ia berkata, Rasulullah SAW. bersabda: ‘Apabila seseorang membicarakan sesuatu kepada orang lain (sambil) menoleh kanan kiri (karena yang dibicarakannya itu rahasia) maka itu amanah (yang harus dijaga)’” (HR Abu Daud 4225) (Labib MZ, 1996a).

Apabila ada orang yang memberitahu sesuatu kemudian orang tersebut pergi atau menoleh ke kanan dan ke kiri sebagai tanda bahwa pesan yang disampaikan tersebut tidak ingin diketahui oleh orang lain, maka itu merupakan bentuk amanah yang harus dijaga kerahasiaannya. Sehingga menjaga rahasia ini wajib dilakukan untuk semua orang.

Rasulullah SAW memberikan sebuah hadis yang diriwayatkan oleh Abu Daud sebagai berikut:

حَدَّثَنَا مُحَمَّدُ بْنُ الْعَلَاءِ وَأَحْمَدُ بْنُ إِبْرَاهِيمَ قَالَ حَدَّثَنَا طَلْقُ بْنُ عَنَامٍ عَنْ شَرِيكَ قَالَ ابْنُ الْعَلَاءِ وَقَيْسٌ عَنْ أَبِي حُصَيْنٍ عَنْ أَبِي صَالِحٍ عَنْ أَبِي هُرَيْرَةَ قَالَ رَسُولُ اللَّهِ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ أَدِّ الْأَمَانَةَ إِلَى مَنْ لَيْسَ بِكَ وَلَا تَخُنْ مَنْ خَانَكَ (رواه أبو داود)

Artinya: “Telah menceritakan kepada kami [Muhammad bin Al ‘Ala] dan [Ahmad bin Ibrahim] mereka berkata; telah menceritakan kepada kami [Thalq bin Ghannam] dari [Syarik] [Ibnu Al ‘Ala] dan [Qais] berkata dari [Abu Hushain] dari [Abu Shalih] dari [Abu Hurairah] ia berkata, “Rasulullahu ‘alaihi wasallam bersabda: “Tunaikanlah amanah kepada orang yang mempercayaimu dan jangan engkau mengkhianati orang yang mengkhianatimu!”” (HR. Abu Daud No. 3068) (Labib MZ, 1996b).

Hadis tersebut menjelaskan bahwa amanah harus dipenuhi oleh seseorang yang diberikan tanggung jawab. Orang yang tidak memenuhi amanah di dunia akan dipertanggungjawabkan di akhirat.

Menurut (Abidin & Khairudin, 2017) amanah seakar dengan kata iman. Salah satu ciri orang beriman adalah melaksanakan amanah dengan sebaik mungkin.

Antara amanah dan iman memiliki keterkaitan yang sangat erat seperti yang terdapat pada (Kadir & Mukti, 2010) bahwa Rasulullah SAW bersabda:

حَلَّتْنَا عَبْدُ الصَّمَدِ ، وَحَسَنُ بْنُ مُوسَى ، قَالَ: حَلَّتْنَا أَبُو هِلَالٍ ، عَنِ قَتَادَةَ ، عَنْ أَنَسٍ ،
 قَالَ: مَا خَطَبْنَا نَبِيًّا صَلَّى عَلَيْهِ وَسَلَّمَ إِلَّا قَالَ: " لَا إِيمَانَ لِمَنْ لَا أَمَانَةَ لَهُ وَلَا دِينَ لِمَنْ لَا
 عَهْدَ لَهُ (رواه مسند احمد)

Artinya: “*Abdushshamad dan Hasan bin Musa menceritakan kepada kami, keduanya berkata: Abu Hilal menceritakan kepada kami, dari Qatadah, dari Anas, ia berkata, “Tidaklah Nabi Muhammad Shallallahu ‘alaihi wa sallam mengkhutbahi kepada kami, kecuali Beliau Shallallahu ‘alaihi wa sallam bersabda: Tidak sempurna keimanan bagi orang yang tidak amanah, dan tidak sempurna agama bagi orang yang tidak menepati janjinya”* (HR. Ahmad No 13132).

Orang beriman akan mendapat rasa aman dan tentram karena ia akan merasakan penjagaan dari Allah SWT. Oleh karena itu, penting bagi seseorang untuk menjaga amanah baik itu terhadap Allah SWT, sesama manusia, ataupun terhadap dirinya sendiri sebagai salah satu bentuk untuk menjaga keimanannya.

2.3 Kajian Topik dengan Teori Pendukung

Seiring dengan perkembangan zaman yang semakin pesat, salah satu dampak signifikan dari kemajuan teknologi ini adalah meningkatnya kasus kejahatan *cyber* yang mengancam keamanan pengguna internet. Meskipun teknologi informasi memberikan kemudahan dalam menyebarkan informasi, namun juga membuka celah untuk penyalahgunaan dan kebocoran data pribadi. Untuk melindungi pesan dan informasi penting, diperlukan penggunaan ilmu kriptografi sebagai metode keamanan yang menggunakan berbagai algoritma sesuai dengan yang dibutuhkan. Dengan menerapkan kriptografi, resiko kebocoran informasi dapat diminimalkan dan hanya dapat diakses oleh pihak yang berwenang.

Penelitian ini membahas tentang pengembangan dari sistem kriptografi yang dapat melindungi informasi dari serangan *post-quantum*. Salah satu metode kriptografi yang dapat digunakan adalah kriptosistem *Niederreiter*, yang menggunakan enkripsi kunci publik. Untuk meningkatkan keamanannya, kriptosistem *Niederreiter* menggunakan implementasi kode Goppa, yang merupakan bagian dari skema keamanannya. Kode Goppa menggunakan polynomial untuk membentuk matriks *parity-check* yang kompleks. Selain itu, konsep teori bilangan juga diterapkan untuk memilih parameter dan parameter kunci yang optimal dalam sistem ini.

BAB III

METODE PENELITIAN

3.1 Jenis Penelitian

Jenis penelitian yang digunakan pada penelitian ini adalah penelitian kualitatif karena penelitian ini menekankan pada deskripsi permasalahan dan menjadikannya dasar dalam pengumpulan data. Metode ini bertujuan untuk mengkaji permasalahan secara mendalam untuk menemukan ide baru dalam pengimplementasian kode Goppa biner pada kriptosistem *Niederreiter*.

3.2 Tahapan Penelitian

Berikut merupakan tahapan-tahapan yang akan digunakan untuk penelitian ini adalah:

3.2.1 Proses Pembentukan Kunci

1. Menentukan *Galois Field* (GF) dari polinomial Goppa $g(x)$ untuk mendapatkan parameter kode Goppa biner;
2. Menghitung matriks *parity check* H dengan ukuran 8×12 untuk sebuah kode Goppa $\Gamma(L, g)$ berdimensi $k = 4$;
3. Memilih matriks permutasi P dengan ukuran 12×12 ;
4. Menentukan matriks *non-singular* S dengan ukuran 8×8 ;
5. Menghitung nilai pembentukan kunci H' sebagai kunci publik berukuran 8×12 ;

$$H' = S \cdot H \cdot P$$

3.2.2 Proses Enkripsi

1. Membuat suatu pesan m dengan panjang n -bit dan bobot *hamming* t sebagai *plaintext*;
2. Mengubah m *plaintext* ke bentuk biner dengan menggunakan kode ASCII;
3. Mengurangkan m *plaintext* menggunakan vektor e *error* dengan bobot *hamming* t ;

$$m' = m - e$$

4. Menghitung *codeword* $C = S \cdot H \cdot P \cdot (m')^T$.

3.2.3 Proses Dekripsi

1. Menghitung invers dari matriks *non-singular* S ;
2. Mengalikan *ciphertext* C_i dengan invers dari matriks *non-singular* S untuk menghasilkan matriks Y_i ;

$$Y_i = S^{-1} \times C_i$$

3. Menghitung vektor z sedemikian hingga $H \times z^T = Y_i$;
4. Menghitung matriks *parity check* H untuk $\Gamma(L, g^2(x))$;
5. Mencari sindrom $s(x)$;
6. Mencari himpunan lokasi *error* sehingga mendapatkan \hat{m} ;
7. Mengalikan matriks \hat{m} dengan matriks permutasi P untuk mengembalikan *ciphertext* ke bentuk aslinya;

$$m_i = \hat{m} \times P$$

8. Kode biner m_i yang diperoleh dikembalikan kedalam bentuk teks berdasarkan Tabel ASCII.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Proses Pembentukan Kunci

Kriptosistem *Niederreiter* merupakan salah satu kriptosistem kunci publik yang berbasis teori kode dan dikategorikan sebagai tingkat keamanan yang paling kuat untuk kriptografi *post-quantum*. Proses pembentukan kunci pada kriptosistem *Niederreiter* menggunakan kode Goppa biner sangat penting untuk menjamin keamanan dan keefektifan sistem kriptografi. Proses pembentukan kunci diawali dengan mencari parameter dari kode Goppa biner untuk menentukan matriks *parity check* H , matriks *non-singular* S , dan matriks permutasi P . Matriks permutasi P dan matriks *non-singular* S yang dibangkitkan secara acak ini digunakan untuk membentuk sebuah kunci H' . Untuk mendapatkan parameter dari kode Goppa biner, dilakukan dengan menggunakan pemilihan polinomial kode Goppa.

4.1.1 Proses Simulasi Pembentukan Kunci pada Kriptosistem *Niederreiter*

Tahap awal dalam sistem kriptosistem *Niederreiter* adalah dilakukan pembentukan kunci. Dipilih lapangan hingga $GF(2^4)$ untuk setiap polinomial tak tereduksi yang berderajat 4. Ukuran lapangan $GF(2^4)$ memberikan jumlah elemen yang cukup dan masih efisien dalam perhitungan untuk mendefinisikan kode Goppa. Untuk mencari elemen primitifnya, dapat dilihat dari polinomial tak tereduksi yang memenuhi $x^{15} = 1$, sehingga $x^{15} - 1$ diperoleh persamaan $x^{15} - 1 = (x + 1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$.

Misal α adalah elemen primitif yang diperoleh dari $x^4 + x + 1$, maka α dapat digunakan untuk membangkitkan sebuah elemen dari F_{2^4} sehingga $GF(2^4) = \{0, \alpha, \alpha^2, \dots, \alpha^{14}\}$. Dari yang telah diperoleh sebelumnya, kemudian elemen tersebut dapat direpresentasikan dari $GF(2^4)$ dengan menggunakan $\alpha^4 = \alpha + 1$.

Tabel 4. 1 Representasi Polinomial $GF(2^4)$

| α_i | Representasi Polinomial | Vektor | $(\alpha_i)^{-1}$ |
|---------------|------------------------------------|---------------|-------------------|
| 0 | 0 | $(0,0,0,0)^T$ | 0 |
| α^0 | 1 | $(1,0,0,0)^T$ | α^{15} |
| α^1 | α | $(0,1,0,0)^T$ | α^{14} |
| α^2 | α^2 | $(0,0,1,0)^T$ | α^{13} |
| α^3 | α^3 | $(0,0,0,1)^T$ | α^{12} |
| α^4 | $1 + \alpha$ | $(1,1,0,0)^T$ | α^{11} |
| α^5 | $\alpha + \alpha^2$ | $(0,1,1,0)^T$ | α^{10} |
| α^6 | $\alpha^2 + \alpha^3$ | $(0,0,1,1)^T$ | α^9 |
| α^7 | $1 + \alpha + \alpha^3$ | $(1,1,0,1)^T$ | α^8 |
| α^8 | $1 + \alpha^2$ | $(1,0,1,0)^T$ | α^7 |
| α^9 | $\alpha + \alpha^3$ | $(0,1,0,1)^T$ | α^6 |
| α^{10} | $1 + \alpha + \alpha^2$ | $(1,1,1,0)^T$ | α^5 |
| α^{11} | $\alpha + \alpha^2 + \alpha^3$ | $(0,1,1,1)^T$ | α^4 |
| α^{12} | $1 + \alpha + \alpha^2 + \alpha^3$ | $(1,1,1,1)^T$ | α^3 |
| α^{13} | $1 + \alpha^2 + \alpha^3$ | $(1,0,1,1)^T$ | α^2 |
| α^{14} | $1 + \alpha^3$ | $(1,0,0,1)^T$ | α |

Sumber: (Singh, 2020)

Didefinisikan $\Gamma(L, g(x))$ kode Goppa dengan polinomial tak tereduksi sesuai Tabel 4.1 yang didefinisikan sebagai

$$\begin{aligned} g(x) &= (x + \alpha)(x + \alpha^{14}) \\ &= x^2 + \alpha^{14}x + \alpha x + 1 \\ &= x^2 + \alpha^7x + 1 \\ L &= \{\alpha^i | 2 \leq i \leq 13\}. \end{aligned}$$

Sehingga untuk kode ini diperoleh $m = 4, n = 12, t = 2, k \geq n - mt \geq 4, d \geq 2t + 1 \geq 5$. Jadi kode ini adalah kode Goppa $\Gamma(L, g(x))$ yang memiliki parameter $[12, \geq 4, \geq 5]$.

Selanjutnya untuk mencari matriks *parity check* H dari kode Goppa $\Gamma(L, (g(x)))$ dengan $g_1 = \alpha^7, g_2 = 1$, dan $\alpha_1 = \alpha^2, \alpha_2 = \alpha^3, \dots, \alpha_{12} = \alpha^{13}$. Faktor $h_i = g(\alpha_i)^{-1}$ dihitung untuk $1 \leq i \leq 12$ dari persamaan $g(x) = x^2 + \alpha^7x + 1$. Untuk melakukan perhitungan vektor biner ini mengacu pada Tabel 2.4.

$$\begin{aligned} h_1 = g(\alpha^2)^{-1} &= ((\alpha^2)^2 + \alpha^7 \cdot \alpha^2 + 1)^{-1} \\ &= (\alpha^4 + \alpha^9 + 1)^{-1} \\ &= ((1,1,0,0)^T + (0,1,0,1)^T + (1,0,0,0)^T)^{-1} \\ &= ((0,0,0,1)^T)^{-1} = (\alpha^3)^{-1} = \alpha^{12} \\ h_2 = g(\alpha^3)^{-1} &= ((\alpha^3)^2 + \alpha^7 \cdot \alpha^3 + 1)^{-1} \\ &= (\alpha^6 + \alpha^{10} + 1)^{-1} \\ &= ((0,0,1,1)^T + (1,1,1,0)^T + (1,0,0,0)^T)^{-1} \\ &= ((0,1,0,1)^T)^{-1} = (\alpha^9)^{-1} = \alpha^6 \end{aligned}$$

$$\begin{aligned}
h_3 = g(\alpha^4)^{-1} &= ((\alpha^4)^2 + \alpha^7 \cdot \alpha^4 + 1)^{-1} \\
&= (\alpha^8 + \alpha^{11} + 1)^{-1} \\
&= ((1,0,1,0)^T + (0,1,1,1)^T + (1,0,0,0)^T)^{-1} \\
&= ((0,1,0,1)^T)^{-1} = (\alpha^9)^{-1} = \alpha^6
\end{aligned}$$

$$\begin{aligned}
h_4 = g(\alpha^5)^{-1} &= ((\alpha^5)^2 + \alpha^7 \cdot \alpha^5 + 1)^{-1} \\
&= (\alpha^{10} + \alpha^{12} + 1)^{-1} \\
&= ((1,1,1,0)^T + (1,1,1,1)^T + (1,0,0,0)^T)^{-1} \\
&= ((1,0,0,1)^T)^{-1} = (\alpha^{14})^{-1} = \alpha
\end{aligned}$$

$$\begin{aligned}
h_5 = g(\alpha^6)^{-1} &= ((\alpha^6)^2 + \alpha^7 \cdot \alpha^6 + 1)^{-1} \\
&= (\alpha^{12} + \alpha^{13} + 1)^{-1} \\
&= ((1,1,1,1)^T + (1,0,1,1)^T + (1,0,0,0)^T)^{-1} \\
&= ((1,1,0,0)^T)^{-1} = (\alpha^4)^{-1} = \alpha^{11}
\end{aligned}$$

$$\begin{aligned}
h_6 = g(\alpha^7)^{-1} &= ((\alpha^7)^2 + \alpha^7 \cdot \alpha^7 + 1)^{-1} \\
&= (\alpha^{14} + \alpha^{14} + 1)^{-1} \\
&= ((1,0,0,1)^T + (1,0,0,1)^T + (1,0,0,0)^T)^{-1} \\
&= ((1,0,0,0)^T)^{-1} = 1
\end{aligned}$$

$$\begin{aligned}
h_7 = g(\alpha^8)^{-1} &= ((\alpha^8)^2 + \alpha^7 \cdot \alpha^8 + 1)^{-1} \\
&= (\alpha^{16} + \alpha^{15} + 1)^{-1} \\
&= ((0,1,0,0)^T + (1,0,0,0)^T + (1,0,0,0)^T)^{-1} \\
&= ((0,1,0,0)^T)^{-1} = (\alpha)^{-1} = \alpha^{14}
\end{aligned}$$

$$\begin{aligned}
h_8 = g(\alpha^9)^{-1} &= ((\alpha^9)^2 + \alpha^7 \cdot \alpha^9 + 1)^{-1} \\
&= (\alpha^{18} + \alpha^{16} + 1)^{-1} \\
&= ((0,0,0,1)^T + (0,1,0,0)^T + (1,0,0,0)^T)^{-1}
\end{aligned}$$

$$\begin{aligned}
&= ((1,1,0,1)^T)^{-1} = (\alpha^7)^{-1} = \alpha^8 \\
h_9 = g(\alpha^{10})^{-1} &= ((\alpha^{10})^2 + \alpha^7 \cdot \alpha^{10} + 1)^{-1} \\
&= (\alpha^{20} + \alpha^{17} + 1)^{-1} \\
&= ((0,1,1,0)^T + (0,0,1,0)^T + (1,0,0,0)^T)^{-1} \\
&= ((1,1,0,0)^T)^{-1} = (\alpha^4)^{-1} = \alpha^{11} \\
h_{10} = g(\alpha^{11})^{-1} &= ((\alpha^{11})^2 + \alpha^7 \cdot \alpha^{11} + 1)^{-1} \\
&= (\alpha^{22} + \alpha^{18} + 1)^{-1} \\
&= ((1,1,0,1)^T + (0,0,0,1)^T + (1,0,0,0)^T)^{-1} \\
&= ((0,1,0,0)^T)^{-1} = (\alpha)^{-1} = \alpha^{14} \\
h_{11} = g(\alpha^{12})^{-1} &= ((\alpha^{12})^2 + \alpha^7 \cdot \alpha^{12} + 1)^{-1} \\
&= (\alpha^{24} + \alpha^{19} + 1)^{-1} \\
&= ((0,1,0,1)^T + (1,1,0,0)^T + (1,0,0,0)^T)^{-1} \\
&= ((0,0,0,1)^T)^{-1} = (\alpha^3)^{-1} = \alpha^{12} \\
h_{12} = g(\alpha^{13})^{-1} &= ((\alpha^{13})^2 + \alpha^7 \cdot \alpha^{13} + 1)^{-1} \\
&= (\alpha^{26} + \alpha^{20} + 1)^{-1} \\
&= ((0,1,1,1)^T + (0,1,1,0)^T + (1,0,0,0)^T)^{-1} \\
&= ((1,0,0,1)^T)^{-1} = (\alpha^{14})^{-1} = \alpha
\end{aligned}$$

Sehingga diperoleh matriks *parity check* H

$$\begin{aligned}
H &= \begin{bmatrix} (\alpha^2 + \alpha^7)h_1 & (\alpha^3 + \alpha^7)h_2 & \dots & (\alpha^{13} + \alpha^7)h_{12} \\ h_1 & h_2 & \dots & h_{12} \end{bmatrix} \\
H &= \begin{bmatrix} (\alpha^2 + \alpha^7)\alpha^{12} & (\alpha^3 + \alpha^7)\alpha^6 & \dots & (\alpha^{13} + \alpha^7)\alpha \\ \alpha^{12} & \alpha^6 & \dots & \alpha \end{bmatrix} \\
H &= \begin{bmatrix} \alpha^9 & \alpha^{10} & \alpha^9 & \alpha^{14} & \alpha^6 & 0 & \alpha^{10} & \alpha^8 & \alpha^2 & \alpha^7 & \alpha^{14} & \alpha^6 \\ \alpha^{12} & \alpha^6 & \alpha^6 & \alpha & \alpha^{11} & 1 & \alpha^{14} & \alpha^8 & \alpha^{11} & \alpha^{14} & \alpha^{12} & \alpha \end{bmatrix}
\end{aligned}$$

Didapatkan matriks *parity check* H dalam bentuk elemen primitif,

selanjutnya ubah matriks tersebut berukuran 8×12 dalam bentuk biner berdasarkan Tabel 4.1 di mana setiap baris pada H dikonversi menjadi 4 baris biner.

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

Kemudian, menentukan matriks *non-singular* S dengan ukuran 8×8 dan matriks permutasi P dengan ukuran 12×12 secara acak. Misalkan,

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

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

Selanjutnya, matriks H' dihitung dengan mengalikan matriks *parity check* H , matriks *non-singular* S , dan matriks permutasi P .

$$H' = S \times H \times P$$

$$\begin{aligned}
&= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \\
&\times \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} \\
&\times \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \\
&= \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}
\end{aligned}$$

Dengan demikian, matriks H' dengan ukuran 8×12 berhasil dibentuk dan digunakan sebagai kunci publik pada proses enkripsi dalam kriptosistem *Niederreiter*.

4.2 Proses Enkripsi

Proses enkripsi menggunakan kriptosistem *Niederreiter* melibatkan tahapan-tahapan yang berbasis pada teori kode linear. Dalam kriptosistem ini, pesan yang akan dienkripsi akan direpresentasikan sebagai vektor biner. Proses ini diawali dengan pemilihan pesan m *plaintext* yang akan dienkripsi, kemudian dikonversi menjadi vektor biner menggunakan kode ASCII dengan panjang n -bit dan bobot *hamming* t . Vektor ini dikurangkan dengan vektor e *error* agar pesan dapat menghasilkan bobot *hamming* t . Selanjutnya, hasil tersebut ditransposekan dan dikalikan dengan kunci publik H' . Hasil dari perkalian ini menghasilkan vektor *ciphertext* C . *Ciphertext* yang telah dihasilkan menjadikan pesan tersebut sulit dibaca oleh pihak yang tidak berwenang.

4.2.1 Proses Simulasi Enkripsi dengan Kriptosistem *Niederreiter*

Pada bagian ini, pengirim mengubah pesan teks ke bentuk biner menggunakan kode ASCII dengan panjang 8 bit. Sebagai contoh, pengirim akan mengirimkan pesan “IBU”, berdasarkan Tabel ASCII didapatkan pesan sebagai berikut:

$$I = [0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1]$$

$$B = [0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0]$$

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

$$IBU = 010010010100001001010101$$

Kemudian membagi kode biner ke beberapa blok m_1 dan m_2 dengan panjang 12 bit. Jika panjang pesan bukan kelipatan 12 bit, maka pesan tersebut akan ditambahkan dengan bit 0 di belakangnya hingga panjang totalnya menjadi

kelipatan 12 bit, sehingga memungkinkan pembagian pesan ke dalam blok-blok dengan panjang 12 bit secara merata.

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

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

Selanjutnya pesan m_i yang telah diubah ke bentuk biner dikurangkan dengan *error* e_i dengan panjang 12 bit dan bobot *hamming* $t = 2$. Sehingga didapatkan nilai m_1' dan m_2' sebagai berikut:

$$m_1' = m_1 - e_1$$

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

$$-[0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0]$$

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

$$m_2' = m_2 - e_2$$

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

$$-[0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0]$$

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

Selanjutnya pesan $(m_1')^T$ dan $(m_2')^T$ dikalikan dengan matriks H' untuk menghasilkan matriks C_i .

$$C_1 = H' \times (m_1')^T$$

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

$$C_2 = H' \times (m'_2)^T$$

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

Sehingga, *chipertext* yang telah didapatkan dari pesan IBU adalah 1010100000100011.

4.3 Proses Dekripsi

Proses dekripsi ini digunakan untuk mengembalikan pesan ke bentuk semula. Proses dekripsi menggunakan kriptosistem *Niederreiter* melibatkan penggunaan kunci privat untuk mengubah pesan tersebut dari *ciphertext* C_1 dan C_2 yang telah dienkripsi dengan menggunakan kunci publik H' . Kemudian mengalikan *invers*

dari matriks *non singular* S^{-1} dengan *ciphertext* C_1 dan C_2 . Kemudian hasil tersebut digunakan untuk mencari vektor z dengan menggunakan rumus $H \times z_i^T = S^{-1} \times C_i$. Selanjutnya, penerima menggunakan algoritma *decoding* untuk mengoreksi kesalahan yang ada pada *ciphertext*. Selanjutnya, penerima mengalikan hasil tersebut dengan matriks permutasi P untuk mendapatkan pesan asli.

4.3.1 Proses Simulasi Dekripsi dengan Kriptosistem *Niederreiter*

Pada bagian ini, penerima mengembalikan *ciphertext* ke pesan semula. Proses dekripsi dapat dilakukan setelah penerima pesan menerima *ciphertext*. Kemudian penerima menghitung nilai *invers* dari matriks *non singular* S^{-1} .

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

Setelah nilai *invers* dari matriks *non-singular* S^{-1} diperoleh, kalikan dengan *ciphertext* C_1 dan C_2 untuk menghasilkan matriks Y_1 dan Y_2 .

$$Y_1 = S^{-1} \times C_1$$

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

$$Y_2 = S^{-1} \times C_2$$

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

Setelah mendapatkan hasil dari Y_1 dan Y_2 , langkah selanjutnya yaitu mencari nilai vektor z .

$$H \times z_i^T = Y_1$$

$$\begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} \times z_1 = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$z_1^T = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

$$z_1 = [0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1]$$

$$H \times z_2^T = Y_2$$

$$\begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} \times z_2 = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$z_2^T = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$z_2 = [0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0]$$

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

$$\hat{H} = \begin{pmatrix} ((\alpha^2)^3 + \alpha^{14}\alpha^2)h_1^2 & ((\alpha^3)^3 + \alpha^{14}\alpha^3)h_2^2 & \dots & ((\alpha^{13})^3 + \alpha^{14}\alpha^{13})h_{12}^2 \\ ((\alpha^2)^2 + \alpha^{14})h_1^2 & ((\alpha^3)^2 + \alpha^{14})h_2^2 & \dots & ((\alpha^{13})^2 + \alpha^{14})h_{12}^2 \\ \alpha^2 h_1^2 & \alpha^3 h_2^2 & \dots & \alpha^{13} h_{12}^2 \\ h_1^2 & h_2^2 & \dots & h_{12}^2 \end{pmatrix}$$

$$\begin{aligned}h_1^2 &= (\alpha^{12})^2 = \alpha^{24} \\ &= \alpha^9\end{aligned}$$

$$\begin{aligned}h_2^2 &= (\alpha^6)^2 \\ &= \alpha^{12}\end{aligned}$$

$$\begin{aligned}h_3^2 &= (\alpha^6)^2 \\ &= \alpha^{12}\end{aligned}$$

$$\begin{aligned}h_4^2 &= (\alpha)^2 \\ &= \alpha^2\end{aligned}$$

$$\begin{aligned}h_5^2 &= (\alpha^{11})^2 = \alpha^{22} \\ &= \alpha^7\end{aligned}$$

$$\begin{aligned}h_6^2 &= (1)^2 \\ &= 1\end{aligned}$$

$$\begin{aligned}h_7^2 &= (\alpha^{14})^2 = \alpha^{28} \\ &= \alpha^{13}\end{aligned}$$

$$\begin{aligned}h_8^2 &= (\alpha^8)^2 = \alpha^{16} \\ &= \alpha\end{aligned}$$

$$\begin{aligned}h_9^2 &= (\alpha^{11})^2 = \alpha^{22} \\ &= \alpha^7\end{aligned}$$

$$\begin{aligned}h_{10}^2 &= (\alpha^{14})^2 = \alpha^{28} \\ &= \alpha^{14}\end{aligned}$$

$$\begin{aligned}h_{11}^2 &= (\alpha^{12})^2 = \alpha^{24} \\ &= \alpha^9\end{aligned}$$

$$\begin{aligned} h_{12}^2 &= (\alpha)^2 \\ &= \alpha^2 \end{aligned}$$

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

Setelah matriks *parity check* \hat{H} diperoleh, selanjutnya mencari *syndrome*

$s(x)$ sebagai berikut:

$$\text{a. } z_1 = [0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1]$$

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

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

$$\begin{aligned} \sigma(x)s(x) &= (x^2 + \sigma_1x + \sigma_0)(\alpha^{10} + \alpha^{12}x + \alpha^9x^2 + \alpha^8x^3) \\ &= (\alpha^{10}x^2 + \alpha^{12}x^3 + \alpha^9x^4 + \alpha^8x^5) \\ &\quad + (\alpha^{10}\sigma_1x + \alpha^{12}\sigma_1x^2 + \alpha^9\sigma_1x^3 + \alpha^8\sigma_1x^4) \\ &\quad + (\alpha^{10}\sigma_0 + \alpha^{12}\sigma_0x + \alpha^9\sigma_0x^2 + \alpha^8\sigma_0x^3) \end{aligned}$$

$$\begin{aligned}
&= \alpha^8 x^5 + (\alpha^9 + \alpha^8 \sigma_1) x^4 + (\alpha^{12} + \alpha^9 \sigma_1 + \alpha^8 \sigma_0) x^3 \\
&\quad + (\alpha^{10} + \alpha^{12} \sigma_1 + \alpha^9 \sigma_0) x^2 + (\alpha^{10} \sigma_1 + \alpha^{12} \sigma_0) x \\
&\quad + \alpha^{10} \sigma_0 \\
&\equiv (\alpha^{12} + \alpha^7 + \alpha^9 \sigma_1 + \alpha^8 \sigma_0) x^3 \\
&\quad + (\alpha^{10} + \alpha^8 + \alpha^{12} \sigma_1 + \alpha^7 \sigma_1 + \alpha^9 \sigma_0) x^2 \\
&\quad + (\alpha^8 + \alpha^{10} \sigma_1 + \alpha^{12} \sigma_0) x + (\alpha^9 + \alpha^8 \sigma_1 + \alpha^{10} \sigma_0) \\
&\equiv (\alpha^2 + \alpha^9 \sigma_1 + \alpha^8 \sigma_0) x^3 + (\alpha + \alpha^2 \sigma_1 + \alpha^9 \sigma_0) x^2 \\
&\quad + (\alpha^8 + \alpha^{10} \sigma_1 + \alpha^{12} \sigma_0) x + (\alpha^9 + \alpha^8 \sigma_1 + \alpha^{10} \sigma_0)
\end{aligned}$$

Kemudian substitusikan persamaan di atas ke

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

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

$$\begin{cases}
\alpha^2 + \alpha^9 \sigma_1 + \alpha^8 \sigma_0 = 0 \\
\alpha + \alpha^2 \sigma_1 + \alpha^9 \sigma_0 = 0 \\
\alpha^8 + \alpha^{10} \sigma_1 + \alpha^{12} \sigma_0 = 0 \\
\alpha^9 + \alpha^8 \sigma_1 + \alpha^{10} \sigma_0 = 0
\end{cases}$$

Didapatkan $\sigma_0 = 1$ dan $\sigma_1 = \alpha^5$, sehingga

$$\sigma(x) = x^2 + \alpha^5 x + 1 = (x + \alpha^6)(x + \alpha^9)$$

Karena $\alpha_5 = \alpha^6$ dan $\alpha_8 = \alpha^9$, maka diperoleh himpunan lokasi *error*nya adalah

$$B = \{i | \sigma(\alpha_i) = 0\} = \{5, 8\}$$

Diperoleh vektor *error* $e' = [0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0]$,

selanjutnya

$$\begin{aligned}
\hat{m}_1 &= z_1 - e' \\
&= [0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1] \\
&\quad - [0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0] \\
&= [0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1]
\end{aligned}$$

b. $z_2 = [0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0]$

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

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

$$\begin{aligned}
\sigma(x)s(x) &= (x^2 + \sigma_1x + \sigma_0)(\alpha + \alpha x + \alpha^{13}x^2 + \alpha^2x^3) \\
&= (\alpha x^2 + \alpha x^3 + \alpha^{13}x^4 + \alpha^2x^5) \\
&\quad + (\alpha\sigma_1x + \alpha\sigma_1x^2 + \alpha^{13}\sigma_1x^3 + \alpha^2\sigma_1x^4) + (\alpha\sigma_0 \\
&\quad + \alpha\sigma_0x + \alpha^{13}\sigma_0x^2 + \alpha^2\sigma_0x^3)
\end{aligned}$$

$$\begin{aligned}
&= \alpha^2 x^5 + (\alpha^{13} + \alpha^2 \sigma_1) x^4 + (\alpha + \alpha^{13} \sigma_1 + \alpha^2 \sigma_0) x^3 \\
&\quad + (\alpha + \alpha \sigma_1 + \alpha^{13} \sigma_0) x^2 + (\alpha \sigma_1 + \alpha \sigma_0) x + \alpha \sigma_0 \\
&\equiv (\alpha + \alpha + \alpha^{13} \sigma_1 + \alpha^2 \sigma_0) x^3 + (\alpha + \alpha^{12} + \alpha \sigma_1 + \alpha \sigma_1 + \alpha^{13} \sigma_0) x^2 \\
&\quad + (\alpha^2 + \alpha \sigma_1 + \alpha \sigma_0) x + (\alpha^{13} + \alpha^2 \sigma_1 + \alpha \sigma_0) \\
&\equiv (\alpha^{13} \sigma_1 + \alpha^2 \sigma_0) x^3 + (\alpha^{13} + \alpha^{13} \sigma_0) x^2 + (\alpha^2 + \alpha \sigma_1 + \alpha \sigma_0) x \\
&\quad + (\alpha^{13} + \alpha^2 \sigma_1 + \alpha \sigma_0)
\end{aligned}$$

Kemudian substitusikan persamaan di atas ke

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

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

$$\begin{cases} \alpha^{13} \sigma_1 + \alpha^2 \sigma_0 = 0 \\ \alpha^{13} + \alpha^{13} \sigma_0 = 0 \\ \alpha^2 + \alpha \sigma_1 + \alpha \sigma_0 = 0 \\ \alpha^{13} + \alpha^2 \sigma_1 + \alpha \sigma_0 = 0 \end{cases}$$

Didapatkan $\sigma_0 = 1$ dan $\sigma_1 = \alpha^5$, sehingga

$$\sigma(x) = x^2 + \alpha^5 x + 1 = (x + \alpha^6)(x + \alpha^9)$$

Karena $\alpha_5 = \alpha^6$ dan $\alpha_8 = \alpha^9$, maka diperoleh himpunan lokasi *error*-nya adalah

$$B = \{i | \sigma(\alpha_i) = 0\} = \{5, 8\}$$

Diperoleh vektor *error* $e' = [0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0]$,

selanjutnya

$$\begin{aligned}
\widehat{m}_2 &= z_1 - e' \\
&= [0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0] \\
&\quad - [0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0] \\
&= [0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0]
\end{aligned}$$

Setelah mendapatkan semua kata kode yang telah dikoreksi, langkah terakhir adalah mengalikan \hat{m}_i dengan matriks permutasi P untuk memperoleh pesan asli sebagai berikut:

$$m_i = \hat{m}_i \times P$$

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

$$\times \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

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

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

$$\times \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

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

Berdasarkan proses dekripsi di atas diperoleh *codeword* yaitu 010010010100001001010101. Untuk mengembalikan ke bentuk teks, perlu membagi pesan biner ke dalam blok-blok dengan panjang 8-bit. Berdasarkan

Tabel ASCII yang terdapat pada lampiran 1, didapatkan $01001001 - 01000010 - 01010101 = \text{IBU}$.

4.4 Analisis Hasil

Berdasarkan pembentukan kunci pada kriptosistem *Niederreiter* menggunakan kode Goppa biner, kunci publik dari matriks H' dengan ukuran 8×12 yang diperoleh melalui tahapan-tahapan yang kompleks dan dirancang untuk memiliki keamanan yang tinggi. Proses ini dimulai dengan menggunakan metode kode Goppa sebagai basis algoritma *decoding* untuk menentukan parameter kunci. Kemudian algoritma ini diterapkan untuk menghasilkan matriks *parity-check* H . Selanjutnya, matriks ini digunakan untuk memperoleh matriks *non-singular* S dan matriks permutasi P , dimana penggunaan matriks *non singular* S menghasilkan kompleksitas struktural yang memperkuat keamanan kunci publik.

Pada proses awal enkripsi, pesan teks diubah menjadi bentuk biner menggunakan Tabel ASCII sepanjang 8-bit kemudian dibagi menjadi beberapa blok dengan panjang 12-bit. Blok-blok ini kemudian diperkuat dengan melakukan pengurangan menggunakan *error*, yang berfungsi untuk meningkatkan keamanan dan membuat kriptografi menjadi lebih sulit dilakukan. Selanjutnya, hasil tersebut dikalikan dengan matriks H' yang berfungsi sebagai kunci publik, sehingga menghasilkan *ciphertext* yang sulit dipahami oleh pihak yang tidak berwenang. Dengan demikian, enkripsi ini menjadi langkah penting dalam menjaga integritas dan kerahasiaan pesan di dalam Kriptosistem *Niederreiter*. Proses yang kompleks dan penuh pertimbangan ini menjadikan Kriptosistem *Niederreiter* sebagai salah satu metode enkripsi yang efektif dalam melindungi data dari ancaman

kriptanalisis.

Proses dekripsi pada kriptosistem *Niederreiter* menggunakan kode Goppa biner terdapat beberapa tahapan yang kompleks untuk mengembalikan pesan yang terenkripsi ke bentuk semula. Setelah menerima *ciphertext*, tahap awal yaitu mengidentifikasi dan menggunakan matriks invers dari matriks *non-singular S* yang sebelumnya dipakai dalam proses pembentukan kunci. Dekripsi dimulai dengan mengalikan setiap blok pesan terenkripsi dengan matriks *invers S* kemudian mencari vektor z untuk menghasilkan vektor sindrom. Kemudian, menghitung sindrom yang digunakan untuk mencerminkan pola *error* dalam pesan terenkripsi dan mendeteksi serta mengidentifikasi *error* yang membantu menemukan polinomial lokasi *error*-nya. Polinomial ini memiliki akar-akar yang menunjukkan posisi bit yang salah dalam vektor biner pesan tersebut. Setelah lokasi *error* ditemukan, dilakukan pengkoreksian *error* pada bit-bit yang terdeteksi. Kemudian, hasil tersebut dikalikan dengan matriks permutasi P untuk mendapatkan pesan asli. Hasil biner tersebut dikembalikan ke bentuk teks berdasarkan Tabel ASCII yang terdapat pada lampiran 1.

Simulasi kode Goppa biner pada kriptosistem *Niederreiter* menunjukkan bahwa proses enkripsi pesan menghasilkan 8-bit di tiap bloknnya. Selain itu, ditunjukkan juga proses mendekripsi *ciphertext* dan koreksi *error* hingga dapat memulihkan pesan semula 12-bit di tiap blok. Pada lampiran 3 dilakukan percobaan dengan kalimat “Semboyan Bhinneka Tunggal Ika” menggunakan Tabel yang ada di lampiran 2 untuk dilakukan proses enkripsi dan dekripsi. Pada proses enkripsi menggunakan *error* yang berbeda disetiap pesannya dan proses ini menghasilkan 18 *ciphertext*. Sedangkan pada proses dekripsi menghasilkan pesan awal yaitu

“Semboyan Bhinneka Tunggal Ika”.

Penelitian ini berhasil menunjukkan bahwa kriptosistem *Niederreiter* mampu menyajikan tahapan-tahapan pengamanan pesan yang kompleks dan kuat. Dalam penelitian ini, melibatkan tahapan-tahapan pengkoreksian *error* dengan kode Goppa yang menunjukkan keberhasilan dalam mengembalikan pesan terenkripsi ke pesan semula.

4.5 Kajian Integrasi Agama

Berdasarkan hasil yang telah diperoleh dari pembahasan, didapatkan suatu kesimpulan bahwa proses tersebut dengan menggunakan kriptosistem *Niederreiter* pada Kode Goppa digunakan untuk memastikan pesan tersebut hanya dapat diakses oleh orang yang berhak menerimanya tanpa mengubah atau menyalahgunakannya. Prinsip menjaga amanah dan integritas pesan mencerminkan nilai kejujuran dan tanggung jawab dalam menyampaikan informasi yang benar. Amanah bukan hanya sekedar menjaga barang maupun benda fisik, namun juga melindungi sebuah informasi yang bersifat pribadi dan rahasia. Penggunaan teknik kriptografi, seperti kriptosistem *Niederreiter* menggunakan kode Goppa merupakan contoh upaya untuk menjaga amanah dengan memastikan bahwa informasi dilindungi dari pihak-pihak yang tidak berwenang. Dalam dunia digital, menjaga kepercayaan ini sangat penting untuk mempertahankan kerahasiaan dan integritas data.

Dalam Al-Qur'an, Allah SWT berfirman:

وَالَّذِينَ هُمْ لِأَمْتِهِمْ وَعَهْدِهِمْ رِعُونَ ۖ

Artinya: “(Termasuk orang yang selamat dari azab adalah) orang-orang yang memelihara amanat dan janji mereka.” (QS. Al-Ma’arij:32) (Lajnah Pentashihan Mushaf Al-Qur’an, 2019c).

Menurut Zubdatut Tafsir, pada ayat tersebut mereka sama sekali tidak melalaikan amanat yang diberikan kepada mereka, serta tidak menyalahi janji yang mereka buat (Al-Asyqor, 2007). Dalam ayat tersebut menekankan pentingnya menjaga amanah dan memenuhi janji yang memiliki relevansi kuat dalam kriptografi. Menjaga amanah dapat diartikan sebagai tanggung jawab untuk menjaga kerahasiaan dan integritas informasi yang dipercayakan. Sama seperti amanah yang tidak boleh disalahgunakan, dalam kriptografi terdapat kunci enkripsi dan data rahasia yang harus dijaga dengan baik agar tidak disalahgunakan oleh pihak yang tidak berwenang. prinsip menjaga amanah ini mencerminkan pentingnya kepercayaan dan tanggung jawab dalam melindungi informasi, yang juga merupakan fondasi dari keamanan *cyber* dan kriptografi modern.

Amanah dalam Islam berkaitan dengan menjaga kepercayaan dan berperilaku jujur. Dalam penerapan Kode Goppa pada kriptosistem *Niederreiter*, kita berupaya memastikan bahwa pesan yang dikirimkan tetap aman dan terlindungi dari pihak yang tidak berwenang serta setiap informasi penting yang telah dikirim dapat diterima secara utuh dan rahasia, mencerminkan tanggung jawab dalam menjaga kerahasiaan informasi tersebut. Hal ini sejalan dengan nilai-nilai amanah yang diajarkan dalam Islam. Beragam teguran untuk menjauhi segala bentuk pelanggaran terhadap amanah juga disampaikan oleh Allah SWT, seperti yang telah diriwayatkan oleh Imam Bukhari, Rasulullah SAW juga bersabda.

عَنْ أَبِي هُرَيْرَةَ قَالَ سَمِعْتُ النَّبِيَّ صَلَّى اللهُ عَلَيْهِ وَسَلَّمَ فِي مَجْلِسٍ يُحَدِّثُ الْقَوْمَ، جَاءَهُ أَعْرَابِيٌّ فَقَالَ: مَتَى السَّاعَةُ؟ فَمَضَى رَسُولُ صَلَّى اللهُ عَلَيْهِ وَسَلَّمَ يُحَدِّثُ، فَقَالَ بَعْضُ الْقَوْمِ: سَمِعَ مَا فَكَّرَهُ مَا قَالَ، وَقَالَ بَعْضُهُمْ: بَلْ لَمْ يَسْمَعْ حَتَّى إِذَا قَضَى حَدِيثَهُ قَالَ: أَيْنَ أَرَاهُ السَّائِلُ عَنِ السَّاعَةِ؟ قَالَ: هَذَا رَسُولٌ، قَالَ: فَإِذَا ضَيَّعَتِ الْأَمَانَةُ فَلَنْتَظِرَ السَّاعَةَ. قَالَ: كَيْفَ إِضَاعَتُهَا رَسُولٌ؟ قَالَ: إِذَا وَبَّدَ الْأَمْرُ إِلَى غَيْرِ أَهْلِهِ فَلَنْتَظِرَ السَّاعَةَ. (أَخْرَجَهُ الْبُخَارِيُّ)

Artinya: “dari Abu Hurairah R.A. berkata: “Pada satu Ketika Rasulullah SAW sedang berbicara dengan orang banyak (memberi pengajian), dan tiba-tiba datang seorang badui menanyakan kepada beliau, ‘Kapan datangnya hari kiamat?’ Akan tetapi Rasulullah SAW terus berbicara. Ada yang berkata ‘Beliau mendengar pertanyaan itu tapi tidak menyukainya’. Orang yang lainnya berkata ‘Beliau tidak mendengarnya’. Setelah Rasulullah SAW selesai berbicara, beliau bertanya, ‘Mana (perlihatkan kepadaku) orang yang bertanya tentang kiamat tadi?’ ‘Aku wahai Rasulullah’, jawab orang tersebut. Beliau pun bersabda, ‘Apabila amanah telah disia-siakan, maka tunggulah datangnya kiamat’. Orang tersebut Kembali bertanya, ‘Bagaimanakah cara disia-siakannya amanah?’ Beliau menjawab, ‘Apabila suatu urusan diserahkan kepada yang bukan ahlinya, maka tunggulah datangnya kiamat’.” (H.R. Imam Bukhari) (Al Albani, 2007).

Dalam hadis tersebut, Rasulullah SAW telah memperingatkan tentang tanda-tanda kehancuran yang akan datang. Salah satunya adalah Ketika amanah disia-siakan, yaitu Ketika suatu tanggung jawab diberikan kepada orang yang tidak berhak untuk menerimanya. Hal ini sangat relevan dengan upaya menjaga kerahasiaan dan integritas pesan dalam kriptografi. Apabila suatu pesan telah diterima oleh pihak yang tidak berwenang, maka akibatnya bisa sangat merugikan seperti mengalami kebocoran informasi yang penting ataupun hilangnya keaslian informasi tersebut.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan rumusan masalah dan hasil dari pembahasan di atas dapat disimpulkan sebagai berikut:

1. Proses pembentukan kunci pada kriptosistem *Niederreiter* menggunakan kode Goppa biner menghasilkan kunci privat dan kunci publik. Kunci privat terdiri dari matriks *non-singular* S berukuran 8×8 , matriks *parity-check* H berukuran 8×12 , dan matriks permutasi P berukuran 12×12 . Sedangkan pada kunci publik menghasilkan matriks H' berukuran 8×12 .
2. Proses enkripsi dalam kriptosistem *Niederreiter* melakukan perubahan pesan menjadi vektor biner dan dikurangkan dengan *error* kemudian dikalikan dengan matriks kunci public H' menghasilkan *ciphertext* 8-bit. Proses ini menjadikan proses enkripsi sebagai langkah penting dalam menjaga kerahasiaan dan keamanan pesan.
3. Proses dekripsi kriptosistem *Niederreiter* melibatkan proses untuk membalikkan enkripsi. Proses ini diawali dengan mengalikan *chipertext* dengan invers matriks *non-singular* S , kemudian *error* dikoreksi dengan memanfaatkan kode Goppa biner. Setelah *error* dikoreksi dan didapatkan vektor kode (\hat{m}) , selanjutnya dikalikan dengan matrik permutasi P untuk mendapatkan pesan semula. Sehingga, pada proses dekripsi ini pesan yang telah terenkripsi kembali ke pesan semula.

Dengan mengimplementasikan kode Goppa biner pada kriptosistem

Niederreiter menunjukkan potensi besar dalam meningkatkan keamanan informasi.

5.2 Saran

Saran untuk penelitian selanjutnya, diharapkan pengamanan pertukaran data dapat diperluas ke bentuk lain seperti gambar, audio, maupun video dengan memanfaatkan algoritma kriptosistem *Niederreiter* menggunakan kode Goppa biner sebagai mekanisme koreksi *error*. Hal ini akan membuka peluang untuk menerapkan sistem keamanan yang lebih luas dan efisien dalam berbagai format data digital, sekaligus mempertahankan tingkat keamanan yang tinggi dalam menghadapi ancaman kriptografi modern, termasuk serangan berbasis komputer kuantum. Dengan demikian, penelitian lebih lanjut diharapkan dapat mengembangkan solusi yang lebih komprehensif dalam bidang keamanan data.

DAFTAR PUSTAKA

- Abidin, Z., & Khairudin, F. (2017). Penafsiran Ayat-Ayat Amanah Dalam Al-Qur'an. *Jurnal Syahadah*, *V*, 120–144.
- Al Albani, M. N. (2007). *Mukhtashar Shahih Bukhari*. Pustaka Azzam.
- Al-Asyqor, M. S. A. (2007). *Zobdat altafser*. Arab Saudi : Kementrian Islam, Dakwah, dan Bimbingan Arab Saudi
- Ariska, B., Suroso, & Endri, J. (2018). Rancangan Kriptografi Hybrid Kombinasi Metode Vigenere Cipher dan Elgamal pada Pengamanan Pesan Rahasia. *Seminar Nasional Inovasi Dan Aplikasi Teknologi Di Industri* , 328–336.
- Baldi, M. (2014). *QC-LDPC Code-Based Cryptography*. Springer International Publishing.
- Danner, J., & Kreuzer, M. (2020). A Fault Attack On The Niederreiter Cryptosystem Using Binary Irreducible Goppa Codes. *Complexity, Cryptology*, *12*(1).
- Fajriyah, N. H., Sari, P., & Nurhidayati, N. (2021). Upaya Penerapan Sifat Wajib Rasul di Era Digital Melalui Pemanfaatan Kriptografi dalam Pengiriman Pesan. *Prosiding Konferensi Integrasi Interkoneksi Islam Dan Sains*, *3*, 37–41.
- Farooq, S., Altaf, A., Iqbal, F., Thompson, E. B., Vargas, D. L. R., Díez, I. de la T., & Ashraf, I. (2023). Resilience Optimization of Post-Quantum Cryptography Key Encapsulation Algorithms. *Sensors (Basel, Switzerland)*, *23*(12), 1–24.
- Ilmiyah, N. F. (2018). Kajian Tentang Kriptosistem McEliece Dalam Menghadapi Tantangan Komputer Kuantum Di Era Revolusi Industri 4.0. *Prosiding Seminar Nasional MIPA*, 216–226.
- Indonesia. Departemen Agama., & Lentera Abadi, PT. (2010). *Mukadimah al-Qur'an dan tafsirnya*. Kementerian Agama Republik Indonesia.
- Kadir, I., & Mukti, M. B. (2010). *Musnad Imam Ahmad*. Pustaka Azzam.
- Labib MZ. (1996a). *Terjemah Ikhtisar Hadits Sunan Abu Daud*. Tiga Dua Surabaya.
- Labib MZ. (1996b). *Terjemah Ikhtisar Hadits Sunan Abu Daud*. Tiga Dua Surabaya.
- Lajnah Pentashihan Mushaf Al-Qur'an. (2016). *Tafsir Ringkas*. Lajnah Pentashihan Mushaf Al-Qur'an.

- Lajnah Pentashihan Mushaf Al-Qur'an. (2019a). *Al-Qur'an dan Terjemah Juz 1-10* (Penyempurnaan 2019). Al-Qur'an dan Terjemahnya.
- Lajnah Pentashihan Mushaf Al-Qur'an. (2019b). *Al-Qur'an dan Terjemah juz 11-20* (Penyempurnaan 2019). Al-Qur'an dan Terjemahnya .
- Lajnah Pentashihan Mushaf Al-Qur'an. (2019c). *Al-Qur'an dan Terjemah juz 21-30* (Penyempurnaan 2019). Al-Qur'an dan Terjemahnya.
- Ling, S., & Xing, C. (2004). *coding theory*. New York : Cambridge University Press
- Musyirifin, Z. (2020). Implementasi Sifat-Sifat Rasulullah dalam Konseling Behavioral. *Al Irsyad, 11*, 151–159.
- Sari, A. (2018). *Karakteristik Bilangan Cokelat*. Bandar Lampung : Matematika
- Singh, H. (2020). *Code based Cryptography: Classic McEliece*.
- Wang, W., Szefer, J., & Niederhagen, R. (2018). *FPGA-based Niederreiter Cryptosystem using Binary Goppa Codes*.

LAMPIRAN

Lampiran 1. Tabel ASCII 8 bit

| <i>Binary</i> | Oct | Dec | Hex | Char |
|---------------|------------|------------|------------|-------------|
| 0100 0001 | 101 | 65 | 41 | A |
| 0100 0010 | 102 | 66 | 42 | B |
| 0100 0011 | 103 | 67 | 43 | C |
| 0100 0100 | 104 | 68 | 44 | D |
| 0100 0101 | 105 | 69 | 45 | E |
| 0100 0110 | 106 | 70 | 46 | F |
| 0100 0111 | 107 | 71 | 47 | G |
| 0100 1000 | 110 | 72 | 48 | H |
| 0100 1001 | 111 | 73 | 49 | I |
| 0100 1010 | 112 | 74 | 4A | J |
| 0100 1011 | 113 | 75 | 4B | K |
| 0100 1100 | 114 | 76 | 4C | L |
| 0100 1101 | 115 | 77 | 4D | M |
| 0100 1110 | 116 | 78 | 4E | N |
| 0100 1111 | 117 | 79 | 4F | O |
| 0101 0000 | 120 | 80 | 50 | P |
| 0101 0001 | 121 | 81 | 51 | Q |
| 0101 0010 | 122 | 82 | 52 | R |
| 0101 0011 | 123 | 83 | 53 | S |
| 0101 0100 | 124 | 84 | 54 | T |
| 0101 0101 | 125 | 85 | 55 | U |
| 0101 0110 | 126 | 86 | 56 | V |
| 0101 0111 | 127 | 87 | 57 | W |
| 0101 1000 | 130 | 88 | 58 | X |
| 0101 1001 | 131 | 89 | 59 | Y |
| 0101 1010 | 132 | 90 | 5A | Z |
| 0110 0001 | 141 | 97 | 61 | a |

| | | | | |
|-----------|-----|-----|----|---|
| 0110 0010 | 142 | 98 | 62 | b |
| 0110 0011 | 143 | 99 | 63 | c |
| 0110 0100 | 144 | 100 | 64 | d |
| 0110 0101 | 145 | 101 | 65 | e |
| 0110 0110 | 146 | 102 | 66 | f |
| 0110 0111 | 147 | 103 | 67 | g |
| 0110 1000 | 150 | 104 | 68 | h |
| 0110 1001 | 151 | 105 | 69 | i |
| 0110 1010 | 152 | 106 | 6A | j |
| 0110 1011 | 153 | 107 | 6B | k |
| 0110 1100 | 154 | 108 | 6C | l |
| 0110 1101 | 155 | 109 | 6D | m |
| 0110 1110 | 156 | 110 | 6E | n |
| 0110 1111 | 157 | 111 | 6F | o |
| 0111 0000 | 160 | 112 | 70 | p |
| 0111 0001 | 161 | 113 | 71 | q |
| 0111 0010 | 162 | 114 | 72 | r |
| 0111 0011 | 163 | 115 | 73 | s |
| 0111 0100 | 164 | 116 | 74 | t |
| 0111 0101 | 165 | 117 | 75 | u |
| 0111 0110 | 166 | 118 | 76 | v |
| 0111 0111 | 167 | 119 | 77 | w |
| 0111 1000 | 170 | 120 | 78 | x |
| 0111 1001 | 171 | 121 | 79 | y |
| 0111 1010 | 172 | 122 | 7A | z |
| 0010 1110 | 056 | 046 | 2E | . |

Lampiran 2. Pesan asli dengan daftar simbol dan kode biner berdasarkan Tabel ASCII

| Pesan | | Semboyan Bhinneka Tunggal Ika | | | |
|--------|------------|-------------------------------|------------|--------|------------|
| Simbol | Kode Biner | Simbol | Kode Biner | Simbol | Kode Biner |
| S | 0101 0011 | h | 0110 1000 | n | 0110 1110 |
| e | 0110 0101 | i | 0110 1001 | g | 0110 0111 |
| m | 0110 1101 | n | 0110 1110 | g | 0110 0111 |
| b | 0110 0010 | n | 0110 1110 | a | 0110 0001 |
| o | 0110 1111 | e | 0110 0101 | l | 0110 1100 |
| y | 0111 1001 | k | 0110 1011 | I | 0100 1001 |
| a | 0110 0001 | a | 0110 0001 | k | 0110 1011 |
| n | 0110 1110 | T | 0101 0100 | a | 0110 0001 |
| B | 0100 0010 | u | 0111 0101 | | |

Lampiran 3. Implementasi kode Goppa biner pada kriptosistem Niederreiter $n = 12$ dan $k = 4$.

| Kunci | |
|-------------------|--|
| $S_{8 \times 8}$ | $S = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$ |
| $H_{8 \times 12}$ | $H = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$ |

| | | | | | | | | | | | | | | | |
|------------------------|--|--|--|--------------------------|--|--|--|-------------------|--|--|--|-----------------|--|--|--|
| $P_{12 \times 12}$ | $P = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$ | | | | | | | | | | | | | | |
| $H' = SHP$ | $= \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$ | | | | | | | | | | | | | | |
| Pesan | | | | Codeword | | | | Pesan | | | | Codeword | | | |
| m_1 | | | | 010100110110 | | | | m_{10} | | | | 010101101011 | | | |
| m_2 | | | | 010101101101 | | | | m_{11} | | | | 011000010101 | | | |
| m_3 | | | | 011000100110 | | | | m_{12} | | | | 010001110101 | | | |
| m_4 | | | | 111101111001 | | | | m_{13} | | | | 011011100110 | | | |
| m_5 | | | | 011000010110 | | | | m_{14} | | | | 011101100111 | | | |
| m_6 | | | | 111001000010 | | | | m_{15} | | | | 011000010110 | | | |
| m_7 | | | | 011010000110 | | | | m_{16} | | | | 110001001001 | | | |
| m_8 | | | | 100101101110 | | | | m_{17} | | | | 011010110110 | | | |
| m_9 | | | | 011011100110 | | | | m_{18} | | | | 000100000000 | | | |
| Proses Enkripsi | | | | | | | | | | | | | | | |
| Pesan | | | | $C_i = H' \times (m')^T$ | | | | Cipherteks | | | | | | | |
| m_1 | | | | 11100010 | | | | C_1 | | | | | | | |
| m_2 | | | | 11100001 | | | | C_2 | | | | | | | |
| m_3 | | | | 01001001 | | | | C_3 | | | | | | | |

| | | |
|------------------------|---------------------------|----------------------|
| m_4 | 10101000 | C_4 |
| m_5 | 01100011 | C_5 |
| m_6 | 00010000 | C_6 |
| m_7 | 00100110 | C_7 |
| m_8 | 10000101 | C_8 |
| m_9 | 10111111 | C_9 |
| m_{10} | 11101110 | C_{10} |
| m_{11} | 01110111 | C_{11} |
| m_{12} | 00010000 | C_{12} |
| m_{13} | 11001100 | C_{13} |
| m_{14} | 01110110 | C_{14} |
| m_{15} | 01100011 | C_{15} |
| m_{16} | 11011000 | C_{16} |
| m_{17} | 01101110 | C_{17} |
| m_{18} | 00111011 | C_{18} |
| Proses Dekripsi | | |
| Cipherteks | $y_i = S^{-1} \times C_i$ | $H \times z^T = y_i$ |
| C_1 | 10000111 | 000011001010 |
| C_2 | 00001100 | 110001001010 |
| C_3 | 01011000 | 001100000010 |
| C_4 | 01010100 | 111010001011 |
| C_5 | 11001111 | 001101000000 |
| C_6 | 11111111 | 100100000001 |
| C_7 | 10111110 | 001000000101 |
| C_8 | 11101101 | 110000101010 |
| C_9 | 10000101 | 100101000110 |
| C_{10} | 10101110 | 110000011010 |
| C_{11} | 10010101 | 000011010000 |
| C_{12} | 11111111 | 100011000010 |
| C_{13} | 10110101 | 001100000111 |

| C_{14} | 00010100 | 101100001011 | |
|-------------------|--|--|--------------|
| C_{15} | 11001111 | 001101000000 | |
| C_{16} | 11101111 | 111000000000 | |
| C_{17} | 01100111 | 001111000010 | |
| C_{18} | 11101001 | 000000100000 | |
| | | | |
| Cipherteks | Decoding (\hat{m}_i) | $m_i = \hat{m}_i \times P$ | Pesan |
| C_1 | 001111001010 | 010100110110 | m_1 |
| C_2 | 111001011010 | 010101101101 | m_2 |
| C_3 | 001101000011 | 011000100110 | m_3 |
| C_4 | 111010111011 | 111101111001 | m_4 |
| C_5 | 001111000001 | 011000010110 | m_5 |
| C_6 | 101100100001 | 111001000010 | m_6 |
| C_7 | 001101000101 | 011010000110 | m_7 |
| C_8 | 110101101010 | 100101101110 | m_8 |
| C_9 | 101101000111 | 011011100110 | m_9 |
| C_{10} | 111100011010 | 010101101011 | m_{10} |
| C_{11} | 001011010001 | 011000010101 | m_{11} |
| C_{12} | 101011010010 | 010001110101 | m_{12} |
| C_{13} | 101101000111 | 011011100110 | m_{13} |
| C_{14} | 101101011011 | 011101100111 | m_{14} |
| C_{15} | 001111000001 | 011000010110 | m_{15} |
| C_{16} | 111000110000 | 110001001001 | m_{16} |
| C_{17} | 001111000111 | 011010110110 | m_{17} |
| C_{18} | 000000001000 | 000100000000 | m_{18} |

| Pesan | Codeword | Kode Biner | Simbol |
|----------------|------------------------------|-------------------|---------------|
| m_1 m_2 | 010100110110 010101101101 | 01010011 | S |
| | | 01100101 | e |
| | | 01101101 | m |

| | | | |
|-----------------------------|------------------------------|-------------------------------|---|
| m_3 m_4 | 011000100110 111101111001 | 01100010 | b |
| | | 01101111 | o |
| | | 01111001 | y |
| m_5 m_6 | 011000010110 111001000010 | 01100001 | a |
| | | 01101110 | n |
| | | 01000010 | B |
| m_7 m_8 | 011010000110 100101101110 | 01101000 | h |
| | | 01101001 | i |
| | | 01101110 | n |
| m_9 m_{10} | 011011100110 010101101011 | 01101110 | n |
| | | 01100101 | e |
| | | 01101011 | k |
| m_{11} m_{12} | 011000010101 010001110101 | 01100001 | a |
| | | 01010100 | T |
| | | 01110101 | u |
| m_{13} m_{14} | 011011100110 011101100111 | 01101110 | n |
| | | 01100111 | g |
| | | 01100111 | g |
| m_{15} m_{16} | 011000010110 110001001001 | 01100001 | a |
| | | 01101100 | l |
| | | 01001001 | I |
| m_{17} m_{18} | 011010110110 000100101110 | 01101011 | k |
| | | 01100001 | a |
| | | | |
| Pesan yang diperoleh | | Semboyan Bhinneka Tunggal Ika | |

RIWAYAT HIDUP



Aldina Laili Chusnia, lahir di Mojokerto pada 05 September 2001. Penulis merupakan anak kedua dari dua bersaudara dari Bapak Pujiono dan Ibu Painah Wati. Selama masa pendidikan, penulis menempuh Pendidikan mulai dari pendidikan dasar di SDN Candiharjo Mojokerto yang lulus pada tahun 2014. Selanjutnya penulis menempuh pendidikan menengah pertama di SMPN 1 Ngoro Mojokerto dan lulus pada tahun 2017. Kemudian melanjutkan pendidikan jenjang menengah atas di SMAN 1 Ngoro Mojokerto sampai tahun 2020. Setelah lulus dari jenjang menengah atas, pada tahun yang sama penulis melanjutkan pendidikan sebagai mahasiswa program studi Matematika di Universitas Islam Negeri Maulana Malik Ibrahim Malang.

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



BUKTI KONSULTASI SKRIPSI

Nama : Aldina Laili Chusnia
NIM : 200601110006
Fakultas/Jurusan : Sains dan Teknologi/Matematika
Judul Skripsi : Implementasi Kode Goppa Biner pada Kriptosistem
Niederreiter
Pembimbing I : Muhammad Khudzaifah, M.Si
Pembimbing II : Erna Herawati, M.Pd

| No | Tanggal | Hal | Tanda Tangan |
|-----|------------------|--------------------------------------|--------------|
| 1. | 19 Februari 2024 | Konsultasi Bab I, II, dan III | 1. |
| 2. | 7 Mei 2024 | Konsultasi Revisi Bab I, II, dan III | 2. |
| 3. | 8 Mei 2024 | Konsultasi Kajian Agama | 3. |
| 4. | 13 Mei 2024 | Konsultasi Revisi Kajian Agama | 4. |
| 5. | 16 Mei 2024 | ACC Kajian Agama Bab I dan II | 5. |
| 6. | 16 Mei 2024 | ACC Bab I, II, dan III | 6. |
| 7. | 8 Juli 2024 | ACC Seminar Proposal | 7. |
| 8. | 22 Juli 2024 | Konsultasi Revisi Seminar Proposal | 8. |
| 9. | 24 Juli 2024 | Konsultasi Bab IV | 9. |
| 10. | 30 Juli 2024 | Konsultasi Bab IV dan V | 10. |
| 11. | 27 Agustus 2024 | Konsultasi Bab IV dan V | 11. |
| 12. | 14 Oktober 2024 | Konsultasi Kajian Agama Bab IV | 12. |
| 13. | 18 Oktober 2024 | ACC Kajian Agama Bab IV | 13. |
| 14. | 29 Oktober 2024 | ACC Bab IV dan V | 14. |
| 15. | 12 November 2024 | ACC Seminar Hasil | 15. |



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

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

Malang, 18 Desember 2024

Mengetahui,

Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc.

NIP. 19741129 200012 2 005