IMPLEMENTASI *MODULE LEARNING WITH ERRORS* PADA PENGAMANAN DATA TRANSAKSI PT. INDONESIA COMNET PLUS SURABAYA

SKRIPSI

OLEH:
RIZA IVANIA INDAH RAVELINA
NIM. 210601110073

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG
2025

IMPLEMENTASI *MODULE LEARNING WITH ERRORS* PADA PENGAMANAN DATA TRANSAKSI PT. INDONESIA COMNET PLUS SURABAYA

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
Riza Ivania Indah Ravelina
NIM. 210601110073

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG
2025

IMPLEMENTASI *MODULE LEARNING WITH ERRORS* PADA PENGAMANAN DATA TRANSAKSI PT. INDONESIA COMNET PLUS SURABAYA

SKRIPSI

Oleh
Riza Ivania Indah Ravelina
NIM. 210601110073

Telah Disetujui Untuk Diuji

Malang, 19 Mei 2025

Dosen Pembimbing I	Dosen Pembimbing II
Muhammad Khudzaifah, M.Si.	Abdul Aziz, M.Si.
NIPPPK. 19900511 202321 1 029	NIP. 19760318 200604 1 002

Mengetahui,
Ketua Program Studi Matematika

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

IMPLEMENTASI *MODULE LEARNING WITH ERRORS* PADA PENGAMANAN DATA TRANSAKSI PT. INDONESIA COMNET PLUS SURABAYA

SKRIPSI

Oleh
Riza Ivania Indah Ravelina
NIM. 210601110073

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

Tanggal 10 Juni 2025

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

Mengetahui,
Ketua Program Studi Matematika

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

PERNYATAAN KEASLIAN TULISAN

Saya bertanda tangan dibawah ini

Nama : Riza Ivania Indah Ravelina

NIM : 210601110073

Program Studi : Matematika

Fakultas : Sains dan Teknologi

Judul Skripsi : Implementasi *Module Learning with Errors* pada Pengamanan Data Transaksi PT. Indonesia Comnet Plus Surabaya

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 halam terakhir. Apabila dikemudian hari terbukti skripsi ini adalah hasil jiplakan atau tiruan, maka saya bersedia menerima sanksi yang berlaku atas perbuatan tersebut.

Malang, 10 Juni 2025

Riza Ivania Indah R.

NIM. 210601110073

MOTO

“Aku memberi lebih untuk yang berarti, dan berjuang keras untuk hidup yang aku impikan”

PERSEMBAHAN

Skripsi ini penulis persembahkan untuk :

Bapak Muhammad Jainul dan Ibu Ruli Erni Astuti yang senantiasa mendoakan dan memberi nasihat serta dukungannya tanpa henti kepada penulis dalam setiap langkahnya.

Kedua kakak saya yaitu Erlian Desy Ririanti dan Andriani Virga Kusumawardani yang senantiasa mendukung penulis.

Keempat keponakan saya yang senantiasa memberikan semangat dan kebahagiaan dalam proses penulisan skripsi

Sahabat dan teman-teman penulis yang memberikan semangat dan bersama-sama berjuang dalam menyelesaikan skripsi.

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji syukur penulis panjatkan ke hadirat Allah SWT atas segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan penelitian dengan judul "Implementasi Module Learning with Errors pada Pengamanan Data Transaksi PT. Indonesia Comnet Plus Surabaya". Shalawat serta salam semoga tetap tercurahkan kepada Baginda Nabi Muhammad SAW yang telah membawakan kabar gembira yakni agama islam sebagai jalan keselamatan dan kebahagiaan dunia dan akhirat.

Penulis menyadari bahwa skripsi ini tidak akan dapat terselesaikan dengan usaha penulis itu sendiri, namun banyak yang sangat berperan dalam proses pengerjaan hingga penulis dapat menyelesaikan proposal ini. Oleh karena itu, dengan segala kerendahan dan ketulusan hari, izinkanlah penulis menghaturkan banyak ucapan terima kasih kepada:

1. Prof. Dr. H. M. Zainuddin, M.A., selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim.
2. Prof. Dr. Hj. Sri Harini, M.Si, selaku dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim.
3. Dr. Elly Susanti, S.Pd., M.Sc, selaku ketua Program Studi Matematika, Universitas Islam Negeri Maulana Malik Ibrahim.
4. Muhammad Khudzaifah, M.Si., selaku dosen pembimbing I atas bimbingan, dukungan, dan arahan yang telah diberikan selama proses penyusunan skripsi ini. Semoga ilmu yang Bapak bagikan menjadi amal jariyah dan senantiasa bermanfaat.
5. Abdul Aziz, M.Si., selaku dosen pembimbing II atas kesabaran, arahan, serta masukan yang berharga dalam proses penyelesaian skripsi ini. Semoga segala bimbingan yang diberikan menjadi pahala dan berkah bagi Bapak.
6. Seluruh dosen Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim
7. Ayah M. Jainul, Ruli Erni Astuti, Kakak Erlian Desy Ririanti dan Kakak Andriani Virga Kusumawardani, serta keluarga besar atas doa, dukungan, dan cinta kasih yang selalu menyertai. Segala bentuk dukungan menjadi

kekuatan dalam menyelesaikan skripsi ini. Semoga segala kebaikan yang telah diberikan senantiasa mendapatkan balasan dari Allah SWT.

8. Teman saya Putri, Mazidah, Rika, Anisa, Tasya, Khurin, Liony, Elen, dan Sabilla yang selalu memberikan dukungan serta kebahagiaan untuk menjadi motivasi penulis selama proses penulisan skripsi ini. Semoga segala kebaikan yang telah diberikan senantiasa mendapatkan balasan dari Allah SWT.
9. Seluruh mahasiswa angkatan 2021 dan teman teman penulis atas kebersamaan, dukungan, serta motivasi yang telah diberikan selama masa studi ini. Kehadiran dan semangat kalian menjadi bagian penting dalam perjalanan ini. Semoga kebersamaan ini terus terjalin dan membawa manfaat bagi kita semua.

Malang, 10 Juni 2025

Riza Ivania Indah Ravelina

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

ABSTRAK

Ravelina, Riza Ivania Indah. 2025. **Implementasi Module Learning With Errors pada Pengamanan Data Transaksi PT. Indonesia Comnet Plus Surabaya.** Skripsi. Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Muhammad Khudzaifah, M.Si. (II) Abdul Aziz, M.Si.

Kata kunci: Kriptografi, Learning with Errors (LWE), Module-LWE, Enkripsi, dekripsi, pengamanan.

Perkembangan komputer kuantum membawa ancaman serius terhadap sistem kriptografi klasik seperti RSA dan ECC karena kemampuannya dalam menyelesaikan persoalan matematika kompleks. Sebagai solusi, kriptografi pasca-kuantum hadir dengan pendekatan baru yang lebih tahan terhadap serangan kuantum. Penelitian ini mengimplementasikan Module Learning With Errors (MLWE) untuk mengamankan data transaksi pada PT. Indonesia Comnet Plus Surabaya. MLWE merupakan generalisasi dari Learning with Errors (LWE) yang memanfaatkan struktur modul dalam ring polinomial, sehingga mampu meningkatkan efisiensi sistem kriptografi tanpa mengorbankan keamanannya. Tujuan dari penelitian ini adalah untuk menerapkan skema MLWE sebagai metode pengamanan data transaksi perusahaan, agar informasi sensitif tidak dapat diakses oleh pihak yang tidak berwenang. Data transaksi dalam bentuk bilangan bulat dikonversi ke bentuk biner, lalu dienkripsi dan didekripsi menggunakan skema MLWE. Hasil penelitian menunjukkan bahwa metode ini mampu mengembalikan data asli secara akurat setelah melalui proses dekripsi, dengan tingkat kesesuaian data mencapai 100%. Selain itu, penelitian ini juga mengusulkan alternatif penyimpanan ciphertext dalam bentuk non-polinomial guna mengurangi penggunaan memori, namun tetap mempertahankan keamanan data.

ABSTRACT

Ravelina, Riza Ivania Indah. 2025. **Implementation of Module Learning With Errors on Securing Transaction Data of PT Indonesia Comnet Plus Surabaya.** Thesis. Department of Mathematics, Faculty of Science and Technology, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Advisor: (I) Muhammad Khudzaifah, M.Si. (II) Abdul Aziz, M.Si.

Keywords: Cryptography, Learning with Errors (LWE), Module-LWE, Encryption, decryption, security.

The advancement of quantum computers poses a serious threat to classical cryptographic systems such as RSA and ECC due to their ability to solve complex mathematical problems efficiently. As a solution, post-quantum cryptography emerges with new approaches that are more resilient against quantum attacks. This research implements the Module Learning With Errors (MLWE) scheme to secure transaction data at PT. Indonesia Comnet Plus Surabaya. MLWE is a generalization of the Learning With Errors (LWE) problem that utilizes module structures within polynomial rings, thereby enhancing the efficiency of cryptographic systems without compromising their security. The aim of this study is to apply the MLWE scheme as a method of securing company transaction data, ensuring that sensitive information cannot be accessed by unauthorized parties. Transaction data in the form of integers is first converted into binary, then encrypted and decrypted using the MLWE scheme. The results show that this method is capable of accurately restoring the original data after the decryption process, achieving a data recovery accuracy of 100%. Additionally, this research proposes an alternative method for storing ciphertext in a non-polynomial format to reduce memory usage, while still maintaining data security.

مستخلص البحث

رافلينا، ريزا إيفانيا إندا. ٢٠٢٥. **تطبيق نمط التعلم بالأخطاء Module Learning With**) (**Errorsفي تأمين بيانات معاملات شركة بي تي إندونيسيا كومنيت بلس سورابايا**. أطروحة. قسم الرياضيات، كلية العلوم والتكنولوجيا، جامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج. المشرفون: (١) محمد خذيفة، ماجستير علوم. (٢) عبد العزيز، ماجستير علوم.

الكلمات الأساسية: التشفير، التعلم بالأخطاء(LWE) ، نمط التعلم بالأخطاء(Module-LWE)، التشفير، فك التشفير، التأمين.

إن تطور الحوسبة الكمومية يشكل تهديدًا خطيرًا لأنظمة التشفير الكلاسيكية مثل RSA و ECC، نظرًا لقدرتها على حل المشكلات الرياضية المعقدة. وكمحاولة لإيجاد حل، يظهر التشفير ما بعد الكمومي بنهج جديد أكثر مقاومة للهجمات الكمومية. يقوم هذا البحث بتطبيق نمط التعلم بالأخطاء Module Learning With) Errors - MLWE)تأمين بيانات المعاملات في شركة بي تي إندونيسيا كومنيت بلس سورابايا. يُعد MLWEتعميمًا للتعلم بالأخطاء (LWE) الذي يستفيد من بنية الوحدة النمطية (module) في حلقة متعددة الحدود(polynomial ring) ، مما يمكنه من زيادة كفاءة نظام التشفير دون التضحية بأمانه

الهدف من هذا البحث هو تطبيق مخطط MLWE كطريقة لتأمين بيانات معاملات الشركة، لضمان عدم وصول المعلومات الحساسة إلى أطراف غير مصرح لها. تم تحويل بيانات المعاملات التي كانت في شكل أعداد صحيحة إلى شكل ثنائي، ثم تم تشفيرها وفك تشفيرها باستخدام مخطط .MLWE أظهرت نتائج البحث أن هذه الطريقة قادرة على استعادة البيانات الأصلية بدقة بعد عملية فك التشفير، بمستوى توافق البيانات يصل إلى ١٠٠%. علاوة على ذلك، يقترح هذا البحث أيضًا بديلاً لتخزين النص المشفر (ciphertext) في شكل غير متعدد الحدود لتقليل استخدام الذاكرة، مع الحفاظ على أمان البيانات.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Saat ini teknologi berkembang secara cepat dan pesat, perkembangan ini terjadi di berbagai aspek kehidupan manusia. Kehadiran teknologi komunikasi dan informasi dengan banyaknya kecanggihan dan kemudahan yang dibawanya mampu mengantar manusia ke sebuah tatanan yang memiliki kualitas dan standar hidup yang lebih baik (Yusniah et al., 2022). Oleh karena itu, penggunaan teknologi harus diimbangi dengan pengetahuan dan etika. Pemahaman terhadap berbagai perkembangan teknologi yang diharapkan masyarakat dapat mengoptimalkannya dengan baik dan etika yang benar tanpa melakukan penyalahgunaan, karena perkembangan teknologi memiliki dampak positif dan negatif. Salah satu kejahatan dalam pencurian data atau kebocoran data dapat diatasi dengan kriptografi (Priliasari, 2023).

Perusahaan yang bergerak dalam bidang telekomunikasi seperti PT. Indonesia Comnet Plus memiliki data yang seharusnya tidak diketahui oleh pihak-pihak yang tidak berwenang, salah satunya adalah data transaksi. Data transaksi memiliki peran krusial dalam operasional bisnis, karena data ini mencakup informasi sensitif seperti detail pelanggan, informasi keuangan, serta data operasional perusahaan yang harus dijaga kerahasiaannya (Priliasari, 2023). Dalam konteks ini, perusahaan membutuhkan sistem keamanan data yang kuat untuk menghindari ancaman yaitu kebocoran data. Salah satu caranya adalah dengan menerapkan algoritma kriptografi *post-quantum*, seperti *Learning with Errors.*

Algoritma ini dirancang untuk memberikan tingkat keamanan yang lebih tinggi dan tahan terhadap serangan teknologi kuantum (Sebastian & Tjahyana, 2020).

Kriptografi pasca-kuantum *(post-quantum)* yang menjanjikan adalah *Learning with Errors* (LWE). Konsep dasar LWE yaitu mengamankan data dengan mendasarkan kekuatan enkripsi pada masalah matematika yang kompleks, yaitu kesulitan memecahkan persamaan linier yang telah ditambahkan dengan gangguan *(errors)* (Sebastian & Tjahyana, 2020). *Learning with Errors* memiliki variasi yang lebih efisien yaitu *Module Learning with Errors* (MLWE) (Boudgoust et al., 2023). Variasi ini menggunakan struktur aljabar modular untuk meningkatkan performa tanpa mengorbankan keamanan. Dalam pengaplikasiannya, MLWE semakin relevan di sektor-sektor yang membutuhkan keamanan tinggi, seperti perusahaan perbankan, pemerintahan, dan telekomunikasi. Dalam konteks ini, PT. Indonesia Comnet Plus sebagai penyedia solusi teknologi informasi dan komunikasi memiliki kebutuhan untuk melindungi data transaksi perusahaan dari ancaman *cyber*. Dengan meningkatnya volume transaksi dan nilai strategis data yang dikelola oleh perusahaan, penerapan metode Kriptografi modern seperti MLWE menjadi langkah strategis untuk memastikan perlindungan yang optimal.

Menjaga kerahasiaan sebuah informasi merupakan hal yang penting, hal ini dapat dilihat pada firman Allah dalam Al-Qur'an surah An-Nisa' (4:58) (Kementerian Agama RI, 2024):

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

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

Ayat ini menjelaskan tentang perintah untuk menyampaikan amanah kepada orang yang dipercaya dan berhak menerimanya, agar amanah yang telah disampaikan tidak diberikan kepada pihak yang seharusnya tidak menerimanya. Dengan latar belakang ini, penelitian ini bertujuan untuk mengimplementasikan *Module Learning with Errors (*MLWE) pada data transaksi PT. Indonesia Comnet Plus Surabaya sebagai studi kasus implementasi MLWE dalam mengamankan data transaksi yang diharapkan memberikan kontribusi bagi pengembangan kriptografi pasca-kuantum di Indonesia. Oleh karena itu, berdasarkan uraian yang disebutkan, maka penulis ingin melakukan penelitian dengan judul "Implementasi *Module Learning With Errors* pada Data Transaksi PT. Indonesia Coment Plus Surabaya".

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah dalam penelitian ini adalah bagaimana hasil implementasi *module learning with errors* pada pengamanan data transaksi PT. Indonesia Comnet Plus Surabaya?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, maka tujuan penelitian yang akan dicapai yaitu untuk memperoleh hasil implementasi *module learning with errors* yang dapat digunakan dalam pengamanan data transaksi dari pihak-pihak yang tidak berwenang mengakses data transaksi di PT. Indonesia Comnet Plus Surabaya.

1.4 Manfaat Penelitian

Berdasarkan tujuan penelitian di atas maka setelah melakukan penelitian diharapkan dapat memberikan manfaat sebagai berikut:

1. Memperkaya pemahaman tentang penggunaan algoritma *Module Learning with Errors* dalam pengolahan data transaksi pada PT. Indonesia Comnet Plus Surabaya.
2. Memberikan informasi kepada pembaca tentang implementasi *Module Learning with Errors* terhadap perkembangan kriptografi kunci publik dalam pengolahan data transaksi pada PT. Indonesia Comnet Plus Surabaya.
3. Memberikan alternatif pengamanan terhadap perusahaan PT. Indonesia Comnet Plus Surabaya dalam pengamanan data transaksi untuk mencegah kebocoran data dari pihak yang tidak berwenang.

1.5 Batasan Masalah

Batasan masalah yang digunakan pada penelitian ini untuk menghindari pembahasan secara meluas adalah data transaksi terkait aktivitas operasional kerjasama oleh perusahaan dan mitra pada PT. Indonesia Comnet Plus Surabaya selama empat tahun terakhir yaitu tahun 2021 hingga 2024. Data yang diamankan merupakan jumlah transaksi pada data tersebut, karena pada perusahaan ini data yang berbentuk angka menjadi data yang dianggap krusial.

Dalam penelitian ini, panjang blok data yang dimisalkan m' berukuran 2×1 bit, sehingga matriks A berukuran 2×2 agar dapat dikalikan dengan data yang akan dienkripsi yaitu vektor m' berukuran 2×1, sehingga operasi pada proses enkripsi dapat terdefinisi secara sistematis. Secara implisit menjamin bahwa submatriks-

submatriks penting dalam A tidak bersifat singular. Determinan dari matriks A tidak diberikan batasan secara eksplisit, namun entri-entri di dalam matriks A tetap dalam operasi modulo q. Batasan ini diperlukan untuk menjamin keberhasilan proses dekripsi dan untuk mempertahankan keamanan skema.

1.6 Definisi Istilah

Terdapat beberapa istilah yang digunakan dalam penelitian ini, yakni sebagai berikut:

1. Kriptografi : Skema yang digunakan untuk pengamanan sebuah data agar tidak dapat terbaca dengan proses enkripsi, dan mengembalikannya ke data semula dengan proses dekripsi.
2. Teori *Ring* : Himpunan dua operasi yaitu penjumlahan dan perkalian yang memenuhi sifat abelian untuk penjumlahan dan distributif untuk perkalian.
3. Teori *Module* : Himpunan M dengan operasi penjumlahan dan perkalian skalar dari ring R.
4. Enkripsi : Proses mengubah data menjadi bentuk kode tertentu agar tidak dapat dibaca oleh pihak yang tidak berwenang.
5. Dekripsi : Proses mengubah data yang telah dienkripsi kembali ke bentuk aslinya.

6.	*Module Learning with Errors*	:	Perluasan dari *Learning with Errors* yang bekerja dalam struktur modul.

BAB II

KAJIAN TEORI

2.1 Teori Pendukung

2.1.1 *Ring*

Ring merupakan struktur aljabar yang unsurnya sebuah himpunan dengan dua operasi. Sebuah himpunan yang dimisalkan R dikatakan *ring* apabila R adalah suatu himpunan tak kosong yang dilengkapi dengan dua buah operasi yakni $+$ (operasi penjumlahan) dan $\cdot$ (operasi perkalian) yang dilambangkan dengan $(R, +, \cdot)$ dan memenuhi aksioma (Rasiman et al., 2018):

1. $(R, +)$ grup abelian
   a. Tertutup, yakni $\forall a, b \in R, a + b \in R$
   b. Asosiatif, yakni $\forall a, b, c \in R, (a + b) + c = a + (b + c)$
   c. Terdapat elemen identitas, yakni $\exists e \in R, \forall a \in R, a + e = e + a = a$
   d. Setiap elemen punya invers, yaitu $\forall a \in R, \exists a^{-1} \in R, a + a^{-1} = a^{-1} + a = e$. Untuk selanjutnya a^{-1} dinamakan invers dari a
   e. Komutatif, yakni $\forall a, b \in R, a + b = b + a$
2. $(R, \cdot)$ semigrup
   a. Tertutup, yakni $\forall a, b \in R, a \cdot b \in R$
   b. Asosiatif, yakni $\forall a, b, c \in R, (a \cdot b) \cdot c = a \cdot (b \cdot c)$
3. Sifat distributif kiri dan distributif kanan, yakni $\forall a, b, c \in R$
   a. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ (distributif kiri)
   b. $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ (distributif kanan)

   Misal R adalah *ring* yang mempunyai elemen identitas terhadap operasi

perkalian yang dinotasikan dengan e_1, maka untuk elemen identitas terhadap suatu operasi perkalian (e_1) dinamakan sebagai elemen satuan. *Ring* R yang memuat elemen satuan dinamakan sebagai ring dengan elemen satuan. Elemen identitas terhadap penjumlahan (dikenal sebagai elemen netral untuk operasi penjumlahan) adalah elemen yang jika ditambahkan ke elemen lain dalam himpunan, tidak mengubah elemen tersebut yang dilambangkan sebagai e.

2.1.2 Modul

Teori Modul adalah cabang aljabar abstrak yang mempelajari tentang generalisasi konsep ruang vektor. Modul menjadi generalisasi dari ruang vektor karena jika *ring* R adalah *field*, maka modul atas R menjadi ruang vektor. Modul memungkinkan bekerja pada struktur yang lebih umum daripada ruang vektor, karena tidak semua struktur aljabar memiliki *field* sebagai basis skalar. Modul mirip dengan ruang vektor, tetapi *field* digantikan oleh *ring*. Oleh karena itu, modul memperluas ruang lingkup ruang vektor ke situasi di mana skalar berasal dari *ring* yang memungkinkan aplikasi dalam berbagai konteks lebih luas. Misal M himpunan tak kosong, R adalah suatu ring. M disebut modul kiri atas ring R yang ditulis $M: R - modul\ kiri$ jika memenuhi aksioma berikut (Pipit Muliyah, et al. 2020):

1. $(M, +)$ merupakan grup komutatif
2. Didefinisikan pemetaan

   $R \times M \to M$

   $(r, m) \to rm$

dan memenuhi:

a. $r(m_1 + m_2) = rm_1 + rm_2$

b. $(r_1 + r_2)m = r_1m + r_2m$

c. $(r_1r_2)m = r_1(r_2m)$

d. $1m = m$

$\forall \mathrm{r}, r_1, r_2 \in R, \forall \mathrm{m}, m_1, m_2 \in M$

Jika M himpunan tak kosong, R adalah suatu ring. M disebut modul kanan atas ring R yang ditulis $M{:}\, R - modul\ kanan$ jika memenuhi aksioma berikut (Pipit Muliyah, et al. 2020):

1. $(M, +)$ merupakan grup komutatif
2. Didefinisikan pemetaan

   $M \times R \to M$

   $(m, r) \to mr$

   dan memenuhi:

   a. $(m_1 + m_2)r = m_1r + m_2r$

   b. $m(r_1 + r_2) = mr_1 + mr_2$

   c. $m(r_1r_2) = (mr_1)r_2$

   d. $m1 = m$

   $\forall \mathrm{r}, r_1, r_2 \in R, \forall \mathrm{m}, m_1, m_2 \in M$

Modul menjadi perumuman dari salah satu konsep aljabar yaitu ruang vektor. Pada modul, syarat skalar diperumum menjadi elemen pada suatu *ring* dan bukan lapangan. Dengan demikian, ruang vektor merupakan suatu kasus khusus dari modul dan karena sifat modul yang lebih luas dari ruang vektor, maka ada berbagai sifat-sifat *trivial* pada ruang vektor menjadi *non-trivial* pada modul (Pipit

Muliyah, et al. 2020). Dengan kata lain, modul adalah versi yang lebih umum dan lebih fleksibel dari ruang vektor.

2.1.3 Kriptografi

Menurut Kromodimoeljo (2009), kriptografi adalah ilmu yang mempelajari tentang mengamankan sebuah informasi dengan menggunakan algoritma tertentu. Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Sedangkan dalam bahasa Yunani, kriptografi berasal dari dua kata, yaitu *crypto* dan *graphia. Crypto* artinya rahasia, dan *graphia* adalah tulisan, sehingga dapat diartikan suatu tulisan yang bersifat rahasia.

Pada jaman Romawi kuno, Julius Caesar telah menggunakan teknik kriptografi yang dijuluki *Caesar cipher* untuk mengirim pesan secara rahasia yang meskipun teknik ini pada saat ini sudah tidak memadai. Sedangkan saat perang dunia kedua, pihak sekutu berhasil memecahkan kode mesin kriptografi Jerman, keberhasilan ini sangat membantu pihak sekutu untuk memenangkan perang. Oleh karena itu, pada sejarah kriptografi banyak orang melihat kriptografi sebagai sesuatu yang penuh dengan misteri.

Seiring perkembangan zaman yang terjadi, kriptografi semakin diperlukan dan kegunaannya semakin diperhitungkan oleh banyak orang yang awalnya menganggap bahwa kriptografi adalah sesuatu yang penuh dengan misteri. Kegunaan dari kriptografi yang terus berkembang adalah mengidentifikasi sebuah pesan, dibuat untuk mengirimkan tanda tangan digital dan menguji keaslian dokumen-dokumen yang perlu dikirimkan. Perkembangan ini terjadi karena

adanya penemuan algoritma-algoritma baru dalam kriptografi. Algoritma-algoritma kriptografi bekerja untuk menyamarkan pesan agar tidak terbaca oleh orang lain. Namun, algoritma kriptografi juga memiliki syarat agar algoritma ini dapat dikatakan aman, syarat-syarat ini antara lain (Haryadi & Ladjamuddin, 2017):

1. Kerahasiaan

   Kerahasiaan menyangkut tentang keamanan privasi orang yang memiliki akses untuk menjalankan teknis sebuah algoritma, dan orang tersebut itu harus menjaga kerahasiaan terhadap teknis yang dipercayakan kepadanya, termasuk data penting yang ada dalam sistem. Oleh karena itu, algoritma yang digunakan dapat menjaga informasi dari orang lain, kecuali orang yang memiliki akses karena dipercaya untuk menjaga dan membuka sebuah data penting.

2. Integritas

   Integritas menyangkut bagaimana menjaga konsistensi, akurasi, serta kepercayaan terhadap data untuk setiap waktu sampai seterusnya sehingga informasi data tidak diubah oleh orang-orang yang tidak bertanggung jawab. Oleh karena itu, sistem yang digunakan harus dapat mendeteksi bahwa tidak adanya manipulasi data yang dilakukan oleh pihak manapun yang tidak memiliki kepentingan.

3. Otentikasi

   Otentikasi memberikan dua layanan, layanan pertama berkaitan dengan identifikasi pada pihak – pihak yang ingin mengakses sistem informasi dengan memberikan jaminan keotentikannya. Layanan kedua untuk menguji

identitas seseorang apabila akan memasuki sebuah sistem.

4. Ketiadaan penyangkalan

   Ketiadaan penyangkalan memberikan cara untuk mencegah terjadinya penyangkalan terhadap suatu aksi yang dilakukan oleh pelaku sistem dari informasi. Ketiadaan penyangkalan memberikan cara untuk membuktikan bahwa suatu dokumen datang dari seseorang tertentu sehingga apabila terdapat seseorang yang mencoba mengakui kepemilikan dokumen tersebut, maka dapat dibuktikan kebenarannya.

Konsep dasar kriptografi yaitu mengenkripsi sebuah data menjadi sesuatu yang sulit dibaca oleh seseorang dan memerlukan proses dekripsi untuk memecahkannya. Proses enkripsi dilakukan menggunakan suatu algoritma dengan beberapa parameter. Sedangkan proses dekripsi menggunakan kunci dekripsi agar mendapatkan kembali data asli. Dalam proses dekripsi, terdapat rahasia yang tidak boleh disebarluaskan ke pihak yang tidak berkepentingan. Rahasia ini terletak pada beberapa parameter yang digunakan, kemudian kunci ditentukan oleh parameter. Parameter yang menentukan kunci dekripsi inilah yang harus dirahasiakan agar data asli tidak dapat terbaca dan proses dekripsi tidak dapat dilakukan selain pihak yang berkepentingan. Berikut skema dari proses kriptografi dapat dilihat pada gambar berikut (Kromodimoeljo, 2009):

Gambar 2.1 Skema Enkripsi dan Dekripsi

Proses enkripsi menerima *input* berupa *plaintext* dan kunci, *plaintext* adalah teks asli dari sebuah pesan, sedangkan kunci yang diinputkan bersama

plaintext adalah kunci yang bersifat rahasia yang memiliki nilai bebas dan menentukan hasil untuk algoritma enkripsi. Hasil ini dinamakan *ciphertext. Ciphertext* akan berbentuk sandi atau pesan yang sulit untuk dibaca. Sedangkan proses dekripsi menerima *input* dari *ciphertext* dan kunci sehingga mendapatkan *output* berupa *plaintext* atau pesan asli.

2.1.4 *Module Learning with Errors*

Masalah kriptografi yang menjadi generalisasi masalah aljabar linier adalah *Learning With Errors* (LWE). Masalah kriptografi ini melibatkan penambahan *errors* atau kesalahan pada persamaan linier berbasis kisi untuk menciptakan asumsi yang sulit dipecahkan. LWE memiliki memiliki versi yang memanfaatkan struktur aljabar *ring* untuk mengurangi ukuran parameter dan mempercepat perhitungan yang dinamakan *Ring Learning with Errors. Ring*-LWE bekerja pada *ideal lattices* yang keamanannya bergantung pada asumsi bahwa masalah-masalah pada *ideal lattices* sama sulitnya dengan masalah pada *arbitrary lattices*. Oleh karena itu, *Module* LWE diusulkan untuk menjembatani permasalahan ini dengan menggeneralisasi LWE ke *module lattices*, yaitu struktur yang berada di antara *arbitrary lattices* dan ideal lattices (Langlois & Stehlé, 2015).

Module Learning With Errors (MLWE) adalah generalisasi dari LWE yang dirancang untuk meningkatkan efisiensi dan fleksibilitas. Dalam MLWE, ruang vektor diperluas dari bilangan Z_q ke modul R_q^d, dimana R adalah *ring* bilangan bulat dalam bidang bilangan aljabar (Boudgoust et al., 2023). *Ring* pada hal ini adalah $R_q = Z_q[x]/(x^n + 1)$ atau *ring* polinomial dengan modulo $x^n + 1$.

Pada MLWE, kesalahan e diambil dari distribusi *Gaussian* yang sesuai dengan ring R_q. Kesalahan ini bertujuan untuk menjamin bahwa MLWE sulit untuk dipecahkan. MLWE memiliki beberapa keunggulan dibandingkan varian LWE lainnya, yaitu (Langlois & Stehlé, 2015):

1. Keamanan lebih kuat

   Module Learning with Errors (MLWE) didasarkan pada masalah *worst-case* pada *module lattices*, yang merupakan generalisasi dari *arbitrary lattice*. Ini berarti keamanan MLWE tidak hanya bergantung pada *ideal lattice* seperti dalam *Ring*-LWE, namun pada dimensi yang lebih tinggi yaitu rank d (*module rank*) yang tetap mempertahankan struktur *ring* aljabar.

2. Fleksibilitas

   Dengan memperkenalkan dimensi tambahan melalui *module lattice*, MLWE memungkinkan parameter yang lebih bervariasi, sehingga dapat disesuaikan untuk berbagai aplikasi kriptografi. Parameter seperti derajat bilangan n dan peringkat modul d dapat disesuaikan untuk mencapai keseimbangan antara keamanan dan efisiensi.

3. Efisiensi

   Module Learning with Errors (MLWE) memungkinkan pengurangan ukuran kunci kriptografi dan peningkatan efisiensi algoritma. Meskipun MLWE menggunakan struktur *module lattices*, skema berbasis MLWE sering kali hanya mengalami perlambatan konstan dibandingkan skema berbasis *Ring*-LWE. Ini membuatnya menarik untuk implementasi praktis.

Module Learning with Errors (MLWE) menjadi salah satu kandidat utama untuk algoritma yang aman terhadap komputer kuantum (Langlois & Stehlé, 2015). Dengan fleksibilitas parmeter, MLWE dapat digunakan untuk merancang sistem yang efisien sekaligus aman. Oleh karena itu, *Module Learning with Errors* (MLWE) menawarkan keseimbangan yang ideal antara efisiensi dan keamanan dalam kriptografi berbasis lattice. Dengan memperluas struktur ke *module lattices*, MLWE menjadi salah satu pendekatan yang menjanjikan dalam era kriptografi post-kuantum.

2.1.5 Kriptografi Kunci Publik

Kriptografi memiliki metode yang menggunakan sepasang kunci yang berbeda tetapi saling terkait, metode ini dinamakan kriptografi kunci publik. Dalam konsep kriptografi kunci publik, pengguna memiliki dua kunci yaitu kunci publik dan kunci privat yang keduanya saling terkait secara sistematis. Kunci publik digunakan untuk enkripsi data dan dapat dibagikan secara bebas ke siapa saja. Sedangkan kunci privat digunakan untuk dekripsi data serta harus dijaga kerahasiaannya oleh pemilik (Lusiana & Handikurniawati, 2010). Konsep ini memungkinkan komunikasi yang aman tanpa perlu berbagi kunci rahasia terlebih dahulu. Kunci publik dapat diakses oleh siapa saja sedangkan kunci privat hanya diketahui oleh pemiliknya untuk mendekripsi pesan. Cara kerja kriptografi kunci publik pesan yang dienkripsi dengan kunci publik hanya dapat didekripsi menggunakan kunci privat yang sesuai. Sebaliknya, data yang dienkripsi dengan kunci privat dapat diverifikasi atau didekripsi dengan kunci publik (Liestyowati, 2020).

Keamanan kriptografi terletak pada sulitnya menemukan kunci privat dari kunci publik, karena bergantung pada masalah matematis yang kompleks. Hal ini mengakibatkan tidak membutuhkan saluran yang aman untuk mendistribusikan kunci publik. Namun, terdapat beberapa hal yang harus diperhatikan saat proses pembangkitan kunci suatu pihak, informasi mengenai pembangkitan kunci tersebut, serta pemulihan dari kebocoran kunci. Hal-hal tersebut perlu diperhatikan agar semua pihak yang terkait dengan sistem kriptografi kunci publik terjamin keamanannya. Kegunaannya yang luas membuat kriptografi kunci publik banyak dipakai dalam banyak aplikasi, khususnya yang berkaitan dengan otentikasi data. Salah satunya dalam *Module Learning with Errors.*

Pembangkitan kunci publik dalam *Module Learning with Errors* menggunakan struktur modul dengan pendekatan vektor atau matriks. Pembangkitan kunci ini diawali dengan memilih beberapa parameter yaitu modulus q, rank modul d, dimensi n. Kunci rahasia s dalam skema MLWE adalah vektor acak yang dipilih dari modul R_q^d. Sedangkan untuk kunci publik, terdiri dari dua elemen, yaitu A merupakan matriks acak yang dipilih dari R_q^d dan b yaitu vektor yang akan dihitung sebagai hasil dari operasi (Langlois & Stehlé, 2015):

$$b = (A \cdot s + e)\ mod\ q \qquad (2.\ 1)$$

di mana:

A : Matriks yang dipilih dari R_q^d berukuran 2×2

s : Vektor yang dipilih dari modul R_q^d berukuran 2×1

e : Vektor yang dipilih dari R_q^m berukuran 2×1

$mod\ q$: Operasi modulo agar perhitungan tetap berada dalam ruang terbatas yang telah ditentukan

Pada skema MLWE, pembangkitan kunci publik dilakukan dengan vektor acak yang bertujuan untuk mengurangi kompleksitas komputasi dan ukuran kunci. Namun, proses ini tetap menjaga keamanan berdasarkan kesulitan memecahkan masalah.

2.1.6 Enkripsi dan Dekripsi

Enkripsi adalah Teknik yang digunakan untuk menjaga kerahasiaan data dengan mengubahnya menjadi format yang hanya dapat dipahami oleh pihak yang memiliki kunci privat. Ini penting dalam konteks keamanan informasi untuk melindungi data yang sensitif. Enkripsi menjadi proses untuk mengacak data menggunakan suatu kunci enkripsi yang tujuannya yaitu data menjadi sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi (Kromodimoeljo, 2009). Dalam kriptografi kunci publik, proses enkripsi dan dekripsi menggunakan sepasang kunci yang saling berkaitan, yaitu kunci publik dan kunci privat. Dengan menggunakan kunci publik, alternatif yang menjanjikan untuk kriptografi pasca-kuantum yang didasari dengan LWE. Pada LWE terdapat beberapa variasi salah satunya adalah MLWE.

Enkripsi MLWE menggunakan struktur modul untuk meningkatkan efisiensi dan fleksibilitas dengan tetap memberikan keamanan berdasarkan reduksi dari *lattice problems*. *Module Learning with Errors* (MLWE) memanfaatkan modul R_q^d, dimana $R_q = R/qR$ dengan $R = \mathbb{Z}[x]/f(x))$ adalah ring polinomial modulo q. Elemen-elemen yang beroperasi yaitu modul diatas *ring* R_q. Dalam prinsip MLWE, terdapat parameter d (*rank* modul) untuk menentukan dimensi yang melibatkan beberapa vektor pada R_q. MLWE bekerja

dengan matriks dan vektor dalam modul dengan menambahkan distribusi kesalahan untuk menyulitkan pemulihan data tanpa kunci rahasia. Oleh karena itu, terdapat cara untuk melakukan proses enkripsi dengan MLWE yaitu (Langlois & Stehle, 2015):

$$v = (r.A + e_1)\ mod\ q \tag{2. 2}$$

$$u = (r.b + e_2 + m')\ mod\ q \tag{2. 3}$$

di mana:

u : *Ciphertext* pertama atau hasil enkripsi data

v : *Ciphertext* kedua atau hasil enkripsi data

A : Matriks yang dipilih dari $R_q^{d\times m}$ berukuran 2×2

r : Matriks yang dipilih dari R_q^m berukuran 2×2

b : Vektor yang diperoleh dari proses $b = A \cdot s + e\ mod\ q$

m' : Data asli yang telah diubah menjadi vektor biner dan akan dienkripsi

e_1 : Matriks yang dipilih dari R_q^m berukuran 2×2

e_2 : Vektor yang dipilih dari R_q^mberukuran 2×1

$mod\ q$: Operasi modulo agar perhitungan tetap berada dalam ruang terbatas

Proses enkripsi pada cara ini akan menghasilkan pasangan (u, v), di mana u adalah vektor di R_q^m dan v adalah elemen di R_q. Sedangkan proses penerima data setelah dienkripsi memerlukan proses untuk mengembalikan *ciphertext* menjadi data asli. Dekripsi adalah proses yang dilakukan menggunakan kunci dekripsi untuk mendapatkan kembali data asli (Kromodimoeljo, 2009). Untuk mendekripsi *ciphertext* pada MLWE (u, v), penerima yang memiliki kunci rahasia s dapat melakukan proses dekripsi untuk mendapatkan data asli kembali dengan

cara (Langlois & Stehlé, 2015):

$$D = (u - v.s)\ mod\ q \quad (2.\ 4)$$

di mana:

D : Hasil dari proses dekripsi

v : *Ciphertext* pertama atau hasil enkripsi data

s : Kunci rahasia yang dipilih secara acak dari modul R_q^d yang berukuran 2×1

u : *Ciphertext* kedua atau hasil enkripsi data

$mod\ q$: Operasi modulo agar perhitungan tetap berada dalam ruang terbatas

Setelah mendapatkan hasil dekripsi (D), penerima harus menjumlahkan tiap koefisien pada vektor polinomial untuk menentukan nilai binernya kembali. Dengan demikian, penerima dapat mendekripsikan *ciphertext* ke data awal.

2.1.7 Data Transaksi

Data transaksi merupakan sebuah komponen dalam perusahaan yang terjadi selama perusahaan tersebut beroperasi pada aktivitas tertentu, yang melibatkan transfer informasi, nilai, atau layanan antar pihak yang berinteraksi (Munanda & Monalisa, 2021). Dalam konteks ini, perusahaan memiliki data transaksi untuk menggambarkan aktivitas dengan pihak mitra. Data ini bisa berisi tentang aktivitas operasional selama bekerjasama, baik dalam bentuk fisik maupun digital. Data transaksi biasanya berisi identitas pihak, waktu transaksi, nilai atau isi dari transaksi dan metadata transaksi. Data transaksi memiliki beberapa karakteristik penting yaitu (Olva et al., 2021):

1. Integritas Data

   Data harus tetap utuh dan tidak boleh dimodifikasi selama proses pengolahan atau pengiriman. Hal ini menunjukkan bahwa keamanan integritas data penting dilakukan untuk menjaga data tetap aman dan terjamin.

2. Keandalan dan Keamanan

   Data transaksi harus dikelola dengan prosedur yang aman dan terkontrol untuk mencegah kehilangan atau kerusakan data. Hal ini dapat dilakukan dengan menggunakan sumber data yang aman dan melakukan *backup* secara rutin.

3. Pemrosesan *Real-Time* dan *Batch*

   Sistem pemrosesan transaksi dapat beroperasi dalam mode *real-time,* di mana setiap transaksi diproses segera setelah diterima, atau dalam mode *batch*, di mana transaksi dikumpulkan dan diproses secara bersamaan pada waktu tertentu.

PT. Indonesia Comnet Plus merupakan perusahaan bergerak di bidang telekomunikasi yang memiliki data transaksi mengenai aktivitas operasional dengan mitra selama kedua pihak bekerjasama. Data ini dianggap sangat penting oleh perusahaan, karena berisi informasi yang sensitif untuk diketahui oleh orang yang tidak berkepentingan. Komponen dari data ini yaitu, nama mitra dan jumlah aktivitas kerjasama antara kedua belah pihak selama 4 tahun terakhir. Oleh karena itu, data ini sebaiknya dilindungi untuk mencegah akses yang dapat dilakukan oleh pihak yang tidak berwenang. Hal ini menunjukkan bahwa data ini perlu dilindungi dengan pengolahan yang benar dan terpercaya seperti kriptografi.

2.2 Kajian Integrasi Topik dengan Al-Quran/Hadits

Pada sub bab 1.1 sebelumnya, telah dijelaskan mengenai perintah untuk menyampaikan amanah kepada orang yang dipercaya dan yang berhak menerimanya, agar amanah yang telah disampaikan tidak diberikan kepada pihak yang seharusnya tidak menerimanya. Amanah dalam konteks ini memiliki arti pada keamanan informasi dengan kriptografi yang memastikan integritas dan kerahasiaan datanya. Oleh karena itu, umat muslim hendaknya melindungi amanat yang telah diterima, dan yang tidak berhak mendapatkan sebuah amanat tidak memiliki akses untuk mengetahui amanat yang telah disampaikan. Sebagaimana yang dijelaskan dalam Surah An-Nur (24:27) (Kementerian Agama RI, 2024):

خَيْرٌ ذٰلِكُمْ اَهْلِهَآ عَلٰى وَتُسَلِّمُوْا تَسْتَأْنِسُوْا حَتّٰى بُيُوْتِكُمْ غَيْرَ بُيُوْتًا تَدْخُلُوْا لَا اٰمَنُوْا الَّذِيْنَ يٰٓاَيُّهَا تَذَكَّرُوْنَ لَعَلَّكُمْ لَّكُمْ

"*Wahai orang-orang yang beriman, janganlah memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. Demikian itu lebih baik bagimu agar kamu mengambil pelajaran.*"

Larangan memasuki wilayah pribadi tanpa izin dalam Surah An-Nur (24:27) dapat dianalogikan dengan amanat tentang perlindungan privasi data dalam dunia digital. Salah satu adab dalam islam yaitu menjaga privasi dan menghormati hak milik orang lain. Allah SWT melarang masuk ke rumah orang lain tanpa izin, menegaskan pentingnya adab, tata krama, dan penghormatan terhadap wilayah pribadi seseorang. Islam mengajarkan bahwa privasi adalah hak yang harus dilindungi, dan ayat ini menjadi panduan langsung tentang bagaimana umat islam harus bersikap dalam interaksi sosial.

Dalam tafsir Ibnu Katsir, Surah An-Nur (24:27) menjelaskan bahwa orang yang beriman kepada Allah dan mengamalkan syariat-Nya, maka janganlah memasuki rumah yang bukan rumah kalian sebelum meminta izin dari penghuninya

untuk memasukinya dan memberi salam kepada penghuninya, serta memiliki adab minta izin yang diperintahkan kepada umat islam lebih baik daripada memasuki rumah secara tiba-tiba. Hal ini bertujuan untuk selalu mengingat apa yang diperintahkan dan mengamalkannya. Tafsir ini menekankan bahwa aturan yang tampaknya sederhana seperti meminta izin dan memberi salam memiliki arti yang mendalam dalam hubungan sosial dan umat muslim. Hal ini bukan hanya soal tata krama, tetapi bagian dari ibadah dan tanda keimanan.

Kesimpulan dari ayat ini menegaskan etika memasuki rumah orang lain. Dalam islam menekankan pentingnya adab dan kesopanan dalam interaksi sosial, termasuk meminta izin sebelum masuk ke dalam rumah orang lain. Hal ini menunjukkan penghormatan terhadap privasi penghuni rumah. Meminta izin adalah cara untuk memastikan kesiapan penghuni rumah menerima tamu, sedangkan salam adalah bentuk penghormatan dan doa untuk penghuni. Etika ini membantu menjaga kehormatan, keharmonisan sosial, dan hubungan baik di tengah masyarakat. Hal ini juga menunjukkan bagaimana islam memperhatikan aspek kehidupan sehari-hari dengan panduan yang mendalam dan bermakna. Oleh karena itu, ayat ini menjadi pengingat untuk selalu menjalankan ajaran Allah dalam kehidupan sehari-hari, termasuk hal-hal kecil.

BAB III

METODE PENELITIAN

3.1 Jenis Penelitian

Penelitian ini menggunakan metode kuantitatif untuk mengolah data transaksi dengan mengimplementasikan *Module Learning with Errors* pada data transaksi PT. Indonesia Comnet Plus Surabaya. Pendekatan kuantitatif bertujuan untuk menganalisis data secara objektif berdasarkan angka dan fakta yang diperoleh dari hasil implementasi. Data yang digunakan merupakan data transaksi kerjasama antara perusahaan PT. Indonesia Comnet Plus dengan mitra selama empat tahun terakhir. Data transaksi ini kemudian diolah menggunakan kriptografi dengan *Module Learning with Errors*. Hasil dari penelitian ini memungkinkan peneliti untuk dapat mengidentifikasi data yang telah terenkripsi dan mengembalikannnya lagi kepada data asli dengan cara dekripsi. Dengan demikian, penelitian ini berkontribusi dalam mengolah data transaksi agar tidak dapat diakses dan terbaca oleh pihak yang tidak berwenang serta penelitian ini dapat digunakan untuk pencegahan pencurian data oleh pihak-pihak yang tidak bertanggungjawab.

3.2 Data dan Sumber Data

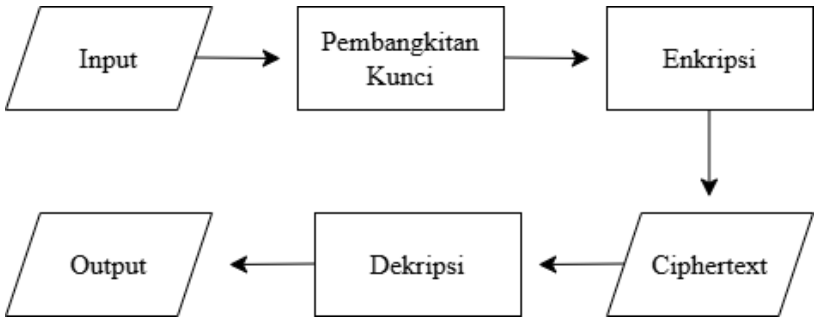
Dalam penelitian ini, data yang digunakan merupakan data sekunder yang diperoleh dari PT. Indonesia Comnet Plus Surabaya. Data ini berisi informasi terkait jumlah transaksi perusahaan dengan mitra selama empat tahun terakhir. Data ini bersifat penting dalam perusahaan. Oleh karena itu, data sebaiknya diolah agar terlindungi dan tidak terbaca data aslinya saat data dikirimkan kepada pihak yang

dituju. Jumlah transaksi empat tahun terakhir pada data ini dituliskan dengan angka yang konstan atau tidak ada variabel seperti x dan y yang belum diketahui nilainya. Selain berisi jumlah transaksi perusahaan dengan mitra, data juga berisi nama-nama mitra yang bekerjasama dengan perusahaan. Selanjutnya, jumlah transaksi pada data ini yang akan dijadikan bahan peneliti untuk diimplementasikan dengan metode yang telah ditentukan. Dengan demikian, data transaksi ini dapat digunakan untuk penelitian ini sebagai dasar yang kuat dalam analisis penelitian.

Penggunaan data sekunder ini memungkinkan penelitian untuk dilakukan dengan lebih efisien dan efektif, mengingat keterbatasan waktu dan sumber daya yang ada. Selain itu, data sekunder yang sudah terverifikasi membantu meningkatkan akurasi dan kredibilitas hasil penelitian.

3.3 Tahapan Penelitian

Berikut alur dari implementasi *Module Learning with Errors* terhadap perkembangan kriptografi kunci publik menggunakan data transaksi pada PT. Indonesia Comnet Plus:



Gambar 3.1 Alur Penelitian

1. Input

   Tahap ini dilakukan pengumpulan data yang akan digunakan dalam penelitian. Data yang digunakan merupakan data sekunder yang diperoleh

dari PT. Indonesia Comnet Plus. Data ini berisi informasi terkait transaksi perusahaan dengan mitra selama empat tahun terakhir, yang mencakup nama-nama mitra dan jumlah transaksi.

2. Pembangkitan Kunci

Pada proses ini dilakukan pembangkitan sepasang kunci publik dan kunci privat. Kunci publik digunakan untuk enkripsi, sedangkan kunci privat digunakan untuk dekripsi. Pembangkitan kunci dilakukan dengan beberapa tahap, yaitu:

a. Pilih kunci privat, misal $s = \begin{bmatrix} x \\ 1 \end{bmatrix}$ berupa vektor acak berukuran 2×1 yang dipilih dari modul R_q^d, dengan $d = 2$, dan $q = 7$

b. Kunci publik terdiri dari dua elemen, yaitu matriks acak berukuran 2×2, misal $A = \begin{bmatrix} x & 1 \\ 2 & x+1 \end{bmatrix}$ dan vektor kunci publik b yang dihasilkan dari $A \cdot s + e \; mod \; q$ (Langlois & Stehle, 2012).

c. Pilih sebarang vektor acak $e = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, e merupakan tambahan *errors* yang dipilih secara acak dan memiliki koefisien yang kecil yaitu berukuran $[-1,0,1]$.

Semua operasi dilakukan di bawah skema *Module*-LWE yaitu modulus $q = 7$. Diperoleh s sebagai kunci privat dan (A, b) sebagai kunci publik yang ditunjukkan kepada orang lain.

3. Enkripsi

Pada proses ini, data diolah dengan menggunakan *Module Learning with Errors*. Tahap yang dilakukan untuk memperoleh *ciphertext* yaitu:

a. Menentukan data yang akan dikirim dan merubah data menjadi bilangan biner $[0, 1]$. Data yang berbentuk akan diubah menjadi bilangan biner. Data dienkripsi per 2-bit. Data asli dimisalkan sebagai m, sedangkan data yang akan digunakan dalam proses enkripsi merupakan data asli yang telah dikalikan dengan $\frac{q}{2}$ dimisalkan dengan m'. Jika $m = 0$ maka $m' = \frac{q}{2} \times 0 \; mod \; q$. Sedangkan jika $m = 1$ maka $m' = \frac{q}{2} \times 1 \; mod \; q$.

b. Menentukan vektor acak dan *noise* yang digunakan dalam proses enkripsi. Pilih sebarang vektor r yang berukuran 2×2 dan e_1 berukuran 2×2, e_2 berukuran 2×1 dan berada dalam R_q^m.

c. Melakukan proses enkripsi yang menghasilkan *ciphertext* berupa (v, u) dengan $v = (r.A + e_1) \; mod \; q$ dan $w = (r.B + e_2 + m')mod \; q$. Semua operasi dilakukan di bawah skema *Module*-LWE yaitu modulus $q = 7$ (Langlois & Stehle, 2012).

4. *Ciphertext*

Setelah melakukan proses enkripsi, diperoleh ciphertext v dan u. Ciphertext v menghasilkan vektor baru berukuran 2×2. Sedangkan ciphertext u menghasilkan vektor baru berukuran 2×1 dan ciphertext (v, u) dilakukan di bawah skema *Module*-LWE yaitu modulus $q = 7$.

5. Dekripsi

Pada proses ini, *ciphertext* yang diperoleh akan dikembalikan ke data aslinya dengan langkah-langkah berikut:

a. Hitung dekripsi dengan $D = (u - s \cdot v) \; mod \; q$ (Langlois & Stehle, 2012).

b. Setelah memperoleh hasil dekripsi D yaitu vektor baru berukuran 2×1, jumlahkan setiap koefisien dari polinomial per baris pada vektor hasil dekripsi tersebut. Jika hasil penjumlahan tersebut lebih dekat ke 0 daripada ke $\frac{q}{2}$ maka data yang diterima adalah 0. Sedangkan jika hasil penjumlahan lebih dekat ke $\frac{q}{2}$ daripada ke 0 maka data yang diterima adalah 1.

c. Susun kembali data dari vektor biner kembali ke data atau karakter semula

d. Konversi vektor biner menjadi bilangan bulat awal atau ke data semula

6. Output

Tahap ini berisi hasil data yang sudah dilakukan dari proses dekripsi pada data transaksi PT. Indonesia Comnet Plus Surabaya. Hasil ini berupa data yang telah kembali ke data awal setelah didekripsi. Hasil yang diperoleh diharapkan membantu untuk pengamanan data pada perusahaan tersebut.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Penjelasan Data

Perusahaan memiliki data yang sangat krusial untuk diketahui oleh orang lain dan mengharuskan perusahaan tersebut memikirkan cara untuk mengamankan sebuah data. Hal ini juga terjadi pada PT. Indonesia Comnet Plus Surabaya yang merupakan anak perusahaan dari PT. PLN (Persero). Perusahaan ini bergerak di bidang layanan jaringan dan telekomunikasi. Data transaksi berjumlah 30 data yang dimiliki oleh perusahaan mengandung jumlah transaksi atau aktivitas yang dilakukan oleh masing-masing mitra kerja perusahaan selama empat tahun, yaitu pada tahun 2021 hingga 2024. Pada data yang akan digunakan untuk penelitian ini selain berisi jumlah transaksi juga berisi inisial mitra. Oleh karena itu, pada penelitian ini proses enkripsi dilakukan untuk jumlah transaksi yang berbentuk bilangan bulat.

PT. Indonesia Comnet Plus Surabaya selalu menganggap bahwa data yang krusial dan wajib untuk dilindungi adalah data yang berisi angka. Oleh karena itu, pada penelitian ini dilakukan pengamanan data dengan *Module Learning With Errors* (MLWE) pada jumlah transaksinya. Dalam penelitian ini, data transaksi yang digunakan merupakan akumulasi dari total transaksi selama empat tahun, bukan data transaksi yang disajikan secara terpisah per tahun. Keputusan ini didasarkan pada pertimbangan dalam konteks pengamanan data dengan objek utama yang perlu dilindungi yaitu informasi yang krusial. Data transaksi kumulatif selama empat tahun dapat mempresentasikan tingkat intensitas dan nilai kerja sama

perusahaan dengan mitra tertentu. Proses pengamanan data dengan menjumlahkan data transaksi dalam satu nilai kumulatif juga dapat menjadikan proses pengamanan data lebih efisien.

Data transaksi kumulatif selama empat tahun dapat mempresentasikan tingkat intensitas dan nilai kerja sama perusahaan dengan mitra tertentu. Informasi ini bersifat strategis dan berpotensi disalahgunakan apabila jatuh ke pihak yang tidak berwenang. Oleh karena itu, menjadikan nilai total transaksi sebagai objek utama enkripsi merupakan langkah yang logis dengan tujuan untuk memberikan perlindungan yang maksimal terhadap informasi sensitif tersebut. Dengan demikian, penggunaan data transaksi dalam bentuk kumulatif adalah langkah strategis yang sesuai dengan tujuan penelitian, serta mendukung efisiensi implementasi kriptografi yang diteliti. Data yang digunakan dalam penelitian ini dapat dilihat pada Tabel 4.1 berikut:

Tabel 4.1 Data Transaksi

Inisial Mitra	Jumlah Transaksi
GMA	504
ACT	282
TAN	250
KLM	190
KDC	157
UNA	156
HGO	149
FIT	136
GSM	121
MDI	102
GAD	98
JGM	89
MIT	84
GTA	79
PAN	77
GDS	70
GLT	67
TDD	63
UKU	52
MBK	49

Inisial Mitra	Jumlah Transaksi
QIM	44
TKW	39
KOJ	34
EFY	30
GDM	27
NAT	23
MBS	21
AMK	11
LIN	7
DAT	2

Data dalam penelitian ini sebanyak 30 data berupa nilai numerik. Data ini berisi jumlah transaksi per mitra yang digunakan sebagai input awal dalam proses pengamanan data menggunakan metode MLWE. Proses pengamanan data dilakukan dengan mengubah data asli menjadi bentuk yang tidak dapat dibaca atau dimengerti oleh pihak lain melalui proses enkripsi. Sebelum proses enkripsi dilakukan, data transaksi dikonversi terlebih dahulu ke dalam bentuk bilangan biner dengan langkah-langkah sebagai berikut:

Misal jumlah transaksi dengan mitra GMA yaitu **504**

$504 \div 2 = 252$, sisa 0

$252 \div 2 = 126$, sisa 0

$126 \div 2 = 63$, sisa 0

$63 \div 2 = 31$, sisa 1

$31 \div 2 = 15$, sisa 1

$15 \div 2 = 7$, sisa 1

$7 \div 2 = 3$, sisa 1

$3 \div 2 = 1$, sisa 1

$1 \div 2 = 0$, sisa 1

Pada proses ini, data akan terus dibagi dengan 2 hingga menghasilkan 0. Jika Panjang bit setelah dilakukan pembagian sebanyak ganjil, maka akan ditambahkan satu bit di depannya dengan angka 0. Berikut adalah data transaksi setelah dikonversi ke bilangan biner.

Tabel 4.2 Data Transaksi setelah Dikonversi

Inisial Mitra	Jumlah Transaksi	Data Biner
GMA	504	0111111000
ACT	282	0100011010
TAN	250	11111010
KLM	190	10111110
KDC	157	10011101
UNA	156	10011100
HGO	149	10010101
FIT	136	10001000
GSM	121	01111001
MDI	102	01100110
GAD	98	01100010
JGM	89	01011001
MIT	84	01010100
GTA	79	01001111
PAN	77	01001101
GDS	70	01000110
GLT	67	01000011
TDD	63	111111
UKU	52	110100
MBK	49	110001
QIM	44	101100
TKW	39	100111
KOJ	34	100010
EFY	30	011110
GDM	27	011011
NAT	23	010111
MBS	21	010101
AMK	11	1011
LIN	7	0111
DAT	2	10

Dengan demikian, input pada proses enkripsi berupa data yang sudah dibinerkan pada tabel 4.2. Penggunaan data dalam bentuk bilangan biner ini bertujuan untuk memastikan data dapat dienkripsi dan didekripsi dengan benar dalam kinerja MLWE.

4.2 Pembangkitan Kunci

Pembangkitan kunci merupakan tahap awal dalam implementasi skema kriptografi berbasis *Learning With Errors* (LWE). Pada tahap ini, dihasilkan pasangan kunci yang terdiri dari kunci publik dan kunci privat yang akan digunakan dalam proses enkripsi dan dekripsi pada data transaksi di PT. Indonesia Comnet Plus Surabaya. Kunci publik digunakan untuk enkripsi, sedangkan kunci privat digunakan untuk dekripsi. Tahap awal pembangkitan kunci adalah memilih vektor acak yang digunakan sebagai kunci privat (s) dari modul R_q^d, d dan q ditentukan terlebih dahulu dalam pemilihan kunci privat (s). Kunci publik pada skema ini terdiri dari dua elemen, yaitu matriks acak A dan vektor kunci publik (b) yang diperoleh dari $(A \cdot s + e)\ mod\ q$. Penambahan *errors* pada penentuan kunci publik (b) dipilih secara acak yang operasi perhitungannya di bawah skema *Module*-LWE bermodulus q. Oleh karena itu, proses ini menjadikan skema kriptografi berbasis *Module*-LWE sebagai metode yang kuat untuk melindungi data.

Kunci privat (s) ditentukan dengan memilih vektor polinomial acak yang terdapat dalam modul R_q^d. Vektor ini merupakan vektor yang berukuran 2×1, yaitu$\begin{bmatrix} x \\ 1 \end{bmatrix}$ dengan $d = 2$ dan $q = 7$. Setelah mendapatkan kunci privat, selanjutnya menentukan kunci publik yang terdiri dari dua elemen. Elemen pertama yaitu matriks polinomial acak yang dipilih dari R_q^d. Matriks ini memiliki ukuran 2×2, yaitu $A = \begin{bmatrix} x & 1 \\ 2 & x+1 \end{bmatrix}$. Dan elemen kedua yaitu vektor kunci publik (b) yang dihasilkan dari $A \cdot s + e\ mod\ q$. Sedangkan penambahan noise (e) dipilih secara acak, vektor ini merupakan vektor yang berukuran 2×1 yaitu $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$. Dengan demikian, kunci publik (b) dapat ditentukan dengan:

$b = (A \cdot s + e)\ mod\ q$

$b = (\begin{bmatrix} x & 1 \\ 2 & x+1 \end{bmatrix} \cdot \begin{bmatrix} x \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix}) mod\ 7$

$b = \begin{bmatrix} x^2 + 1 \\ 3x + 2 \end{bmatrix}$

Pada proses ini, diperoleh kunci publik (A, b) yaitu $(\begin{bmatrix} x & 1 \\ 2 & x+1 \end{bmatrix}, \begin{bmatrix} x^2 + 1 \\ 3x + 2 \end{bmatrix})$. Kunci publik yang telah diperoleh akan digunakan pada proses enkripsi dan dekripsi untuk pengamanan sebuah data.

4.3 Proses Enkripsi

Proses enkripsi pada skema *Module Learning with Errors* dilakukan oleh pengirim menggunakan kunci publik (A, b), sehingga menghasilkan vektor polinomial pada *ciphertext* dan membuat data sulit untuk dibaca oleh pihak yang tidak berwenang untuk mengaksesnya. Proses enkripsi pada MLWE menghasilkan dua *ciphertext* yang setiap *ciphertext*nya ditambahkan noise acak untuk menambahkan keamanan dan kerahasiaan data dalam skema MLWE.

Data yang akan dienkripsi berbentuk bilangan bulat dan dikonversi ke dalam bentuk kode biner dengan cara membagi bilangan bulat secara terus menerus dengan 2, kemudian melihat sisa pembagiannya pada setiap tahap pembagian hingga akhir. Selanjutnya, dipilih vektor polinomial acak (r) berukuran 2×2, vektor polinomial *noise* e_1 berukuran 2×2, serta vektor polinomial *noise* e_2 berukuran 2×1. Pada *noise* e_1 dan e_2, koefisien yang digunakan bernilai kecil, yaitu $[-1,0,1]$. Data yang telah dikonversi ke dalam kode biner kemudian dikelompokkan setiap dua bit untuk proses enkripsi dan diubah menjadi vektor berukuran 2×1. Dengan demikian, *ciphertext* yang diperoleh untuk setiap dua bit

atau setiap vektor dinyatakan sebagai $C_i = (v_i, u_i)$, dengan $v_i = (r.A + e_1)\ mod\ q$ dan $u_i = (r.B + e_2 + m')\ mod\ q$ dengan v_i merupakan sebuah vektor polinomial berukuran 2×2 dan vektor polinomial u_i berukuran 2×1. Nilai vektor polinomial acak r harus berbeda dalam tiap proses enkripsi per bit. Sedangkan nilai *noise* e_1, e_2 bisa sama. Setelah itu, menggunakan kunci publik yang diperoleh dari pembangkitan kunci dengan kunci privat pada setiap proses enkripsi untuk mendapatkan *ciphertext.*

Proses enkripsi dimulai dengan mengkonversi bilangan bulat ke kode biner. Data yang telah dikonversi menjadi bilangan biner dapat dilihat pada Lampiran 2. Pada data yang memiliki panjang bit ganjil, maka akan ditambah satu bit di depan dengan angka 0, untuk memudahkan proses enkripsi dan tidak merubah nilai data awal saat didekripsi kembali. Data dienkripsi satu persatu setiap jumlah transaksi mitra dengan perusahaan, sehingga mendapatkan hasil enkripsi. Proses enkripsi untuk pengamanan data transaksi PT. Indonesia Comnet Plus dapat dilihat pada proses berikut:

Misal data asli adalah **504**, maka binernya adalah 0111111000. Bilangan biner ini didapat dari hasil membagi bilangan bulat secara terus menerus dengan 2, dan melihat sisa pembagiannya pada setiap tahap pembagian hingga akhir. Sehingga, data **504** dalam bentuk vektor biner adalah:

$$m_{biner} = [0\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 0]$$

Diambil per 2 bit dari data yang telah dibinerkan atau m_{biner}, data ini akan membentuk sebuah vektor 2×1. Setelah membentuk vektor 2×1, untuk melakukan proses enkripsi, m akan dikalikan dengan $\frac{q}{2}$ dengan tujuan memastikan pesan dapat dipresentasikan secara aman dalam ruang modulus dan tetap

mempertahankan kemungkinan dekripsi yang benar walau ada noise. Berikut adalah proses enkripsi MLWE:

$m_1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

$m'_1 = \frac{q}{2} \times m \; mod \; q = \frac{7}{2} \times \begin{bmatrix} 0 \\ 1 \end{bmatrix} \; mod \; 7 = \begin{bmatrix} 0 \\ 3 \end{bmatrix}$

$r = \begin{bmatrix} 2 & x+1 \\ x & 2x \end{bmatrix}$

$e_1 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, e_2 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

$v_1 = (r.A + e_1) mod \; 7 = (\begin{bmatrix} 2 & x+1 \\ x & 2x \end{bmatrix} . \begin{bmatrix} x & 1 \\ 2 & x+1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}) mod \; 7$

$$= \begin{bmatrix} 4x+3 & 3+x^2+2x \\ x^2+4x & 2x^2+3x+6 \end{bmatrix}$$

$u_1 = (r.B + e_2 + m'_1) mod \; 7 = (\begin{bmatrix} 2 & x+1 \\ x & 2x \end{bmatrix} . \begin{bmatrix} x^2+1 \\ 3x+2 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 3 \end{bmatrix}) mod \; 7$

$$= \begin{bmatrix} 5x^2+5x+5 \\ x^3+5x+6x^2+3 \end{bmatrix}$$

Jadi, chipertext $(v_1, u_1) = \left(\begin{bmatrix} 4x+3 & 3+x^2+2x \\ x^2+4x & 2x^2+3x+6 \end{bmatrix}, \begin{bmatrix} 5x^2+5x+5 \\ x^3+5x+6x^2+3 \end{bmatrix} \right)$

$m_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$

$m'_2 = \frac{q}{2} \times m \; mod \; q = \frac{7}{2} \times \begin{bmatrix} 1 \\ 1 \end{bmatrix} \; mod \; 7 = \begin{bmatrix} 3 \\ 3 \end{bmatrix}$

$r = \begin{bmatrix} 0 & x \\ x & 1 \end{bmatrix}$

$e_1 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, e_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

$v_2 = (r.A + e_1) mod \; 7 = (\begin{bmatrix} 0 & x \\ x & 1 \end{bmatrix} . \begin{bmatrix} x & 1 \\ 2 & x+1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}) mod \; 7$

$$= \begin{bmatrix} 2x & x^2+x \\ x^2+2 & 2x+1 \end{bmatrix}$$

$u_2 = (r.B + e_2 + m'_2) mod \; 7 = (\begin{bmatrix} 0 & x \\ x & 1 \end{bmatrix} . \begin{bmatrix} x^2+1 \\ 3x+2 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 3 \\ 3 \end{bmatrix}) mod \; 7$

$$= \begin{bmatrix} 3x^2 + 2x + 3 \\ x^3 + 4x + 6 \end{bmatrix}$$

Jadi, chipertext $(v_2, u_2) = \left(\begin{bmatrix} 2x & x^2 + x \\ x^2 + 2 & 2x + 1 \end{bmatrix}, \begin{bmatrix} 3x^2 + 2x + 3 \\ x^3 + 4x + 6 \end{bmatrix} \right)$

$m_3 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$

$m'_3 = \frac{q}{2} \times m \bmod q = \frac{7}{2} \times \begin{bmatrix} 1 \\ 1 \end{bmatrix} \bmod 7 = \begin{bmatrix} 3 \\ 3 \end{bmatrix}$

$r = \begin{bmatrix} x & 0 \\ 2x & 1 \end{bmatrix}$

$e_1 = \begin{bmatrix} 0 & -1 \\ 0 & 0 \end{bmatrix}, e_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

$v_3 = (r.A + e_1) mod\ 7 = (\begin{bmatrix} x & 0 \\ 2x & 1 \end{bmatrix} . \begin{bmatrix} x & 1 \\ 2 & x + 1 \end{bmatrix} + \begin{bmatrix} 0 & -1 \\ 0 & 0 \end{bmatrix}) mod\ 7$

$$= \begin{bmatrix} x^2 & x + 6 \\ 2x^2 + 2 & 3x + 1 \end{bmatrix}$$

$u_3 = (r.B + e_2 + m'_3) mod\ 7 = (\begin{bmatrix} x & 0 \\ 2x & 1 \end{bmatrix} . \begin{bmatrix} x^2 + 1 \\ 3x + 2 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 3 \\ 3 \end{bmatrix}) mod\ 7$

$$= \begin{bmatrix} x^3 + x + 3 \\ 2x^3 + 5x + 6 \end{bmatrix}$$

Jadi, chipertext $(v_3, u_3) = \left(\begin{bmatrix} x^2 & x + 6 \\ 2x^2 + 2 & 3x + 1 \end{bmatrix}, \begin{bmatrix} x^3 + x + 3 \\ 2x^3 + 5x + 6 \end{bmatrix} \right)$

$m_4 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

$m'_4 = \frac{q}{2} \times m \bmod q = \frac{7}{2} \times \begin{bmatrix} 1 \\ 0 \end{bmatrix} \bmod 7 = \begin{bmatrix} 3 \\ 0 \end{bmatrix}$

$r = \begin{bmatrix} 1 & 0 \\ x & 2x \end{bmatrix}$

$e_1 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, e_2 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

$v_4 = (r.A + e_1) mod\ 7 = (\begin{bmatrix} 1 & 0 \\ x & 2x \end{bmatrix} . \begin{bmatrix} x & 1 \\ 2 & x + 1 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}) mod\ 7$

$$= \begin{bmatrix} x & 2 \\ x^2 + 4x & 3x + 2x^2 \end{bmatrix}$$

$$u_4 = (r.B + e_2 + m'_4) mod\ 7 = (\begin{bmatrix}1 & 0\\ x & 2x\end{bmatrix}.\begin{bmatrix}x^2+1\\ 3x+2\end{bmatrix} + \begin{bmatrix}1\\0\end{bmatrix} + \begin{bmatrix}3\\0\end{bmatrix}) mod\ 7$$

$$= \begin{bmatrix} x^2+5 \\ x^3+6x^2+5x \end{bmatrix}$$

Jadi, chipertext $(v_4, u_4) = \left(\begin{bmatrix} x & 2 \\ x^2+4x & 3x+2x^2 \end{bmatrix}, \begin{bmatrix} x^2+5 \\ x^3+6x^2+5x \end{bmatrix}\right)$

$m_5 = \begin{bmatrix}0\\0\end{bmatrix}$

$m'_5 = \frac{q}{2} \times m\ mod\ q = \frac{7}{2} \times \begin{bmatrix}0\\0\end{bmatrix}\ mod\ 7 = \begin{bmatrix}0\\0\end{bmatrix}$

$r = \begin{bmatrix}2 & x\\ x & 2x\end{bmatrix}$

$e_1 = \begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}, e_2 = \begin{bmatrix}1\\0\end{bmatrix}$

$$v_5 = (r.A + e_1) mod\ 7 = (\begin{bmatrix}2 & x\\ x & 2x\end{bmatrix}.\begin{bmatrix}x & 1\\ 2 & x+1\end{bmatrix} + \begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}) mod\ 7$$

$$= \begin{bmatrix} 4x+1 & x^2+x+2 \\ x^2+4x & 2x^2+3x \end{bmatrix}$$

$$u_5 = (r.B + e_2 + m'_5) mod\ 7 = (\begin{bmatrix}2 & x\\ x & 2x\end{bmatrix}.\begin{bmatrix}x^2+1\\ 3x+2\end{bmatrix} + \begin{bmatrix}1\\0\end{bmatrix} + \begin{bmatrix}0\\0\end{bmatrix}) mod\ 7$$

$$= \begin{bmatrix} 5x^2+2x+3 \\ x^3+6x^2+5x \end{bmatrix}$$

Jadi, chipertext $(v_5, u_5) = \left(\begin{bmatrix} 4x+1 & x^2+x+2 \\ x^2+4x & 2x^2+3x \end{bmatrix}, \begin{bmatrix} 5x^2+2x+3 \\ x^3+6x^2+5x \end{bmatrix}\right)$

Dari proses enkripsi, menghasilkan *chipertext* untuk tiap datanya dapat dilihat pada Lampiran 1. Pada Lampiran 1 dapat dilihat bahwa setiap data asli yang telah dienkripsi akan menghasilkan beberapa *chipertext* yang berbeda. Dari *chipertext* ini terdiri dari sepasang *chipertext* v dan *chipertext* u yang berbentuk polinomial. *Chipertext* ini diperoleh dari proses enkripsi yang membagi panjang bit dari data asli menjadi per-2 bit untuk proses enkripsi. Untuk mengurangi penyimpanannya yang berbentuk polinomal, maka pada penelitian ini terdapat alternatif

pemyimpanan pada database berupa koefisien pada *chipertext.*

4.4 Proses Dekripsi

Proses dekripsi pada algoritma *Module Learning with Errors* (MLWE) yang dilakukan oleh pihak penerima data menggunakan kunci rahasia s dan dilakukan per-2 bit. Setelah didapatkan chipertext (v, u) oleh pihak penerima, data asli dapat ditemukan kembali dengan persamaan $(u_i - v_i.s)\ mod\ q$. Dari persamaan tersebut, akan didapatkan sebuah vektor polinomial berukuran 2×1 yang kemudian dijumlahkan pada setiap baris vektor polinomial dari proses dekripsi tersebut. Jika hasil penjumlahannya lebih dekat ke 0 daripada $\frac{7}{2}$, maka data yang didapatkan adalah 0. Sebaliknya, jika hasil penjumlahannya lebih dekat ke $\frac{7}{2}$ daripada ke 0, maka data yang didapatkan adalah 1.

Proses dekripsi dimulai oleh pihak penerima data dengan menerima *chipertext*. Selanjutnya dengan menggunakan kunci privat $s = \begin{bmatrix} x \\ 1 \end{bmatrix}$, dengan menggunakan $D_i = (u_i - v_i.s)\ mod\ q$. Operasi modulo digunakan untuk memastikan hasil perhitungan tetap berada dalam batas nilai yang diizinkan, yaitu antara 0 hingga $q - 1$. Setelah ciphertext dikurangi dengan komponen kunci rahasia, hasilnya di-*reduce* dengan modulo $q$untuk menyesuaikan kembali nilai yang mungkin keluar dari batas karena penjumlahan atau pengurangan sebelumnya. Proses ini memungkinkan sistem tetap akurat meskipun terjadi gangguan kecil selama transmisi data. Hal ini penting agar pesan terenkripsi tetap dapat dikenali meskipun telah tercampur dengan noise. Berikut proses dekripsi untuk mengembalikan *chipertext* ke data asli:

$$D_1 = (u_1 - v_1.s)\ mod\ 7 = \begin{bmatrix} 5x^2+5x+5 \\ x^3+5x+6x^2+3 \end{bmatrix} - \begin{bmatrix} 4x+3 & 3+x^2+2x \\ x^2+4x & 2x^2+3x+6 \end{bmatrix}.\begin{bmatrix} x \\ 1 \end{bmatrix}$$

$$= \begin{bmatrix} 2 \\ 2x+4 \end{bmatrix}$$

$$D_2 = (u_2 - v_2.s)\ mod\ 7 = \begin{bmatrix} 3x^2+2x+3 \\ x^3+4x+6 \end{bmatrix} - \begin{bmatrix} 2x & x^2+x \\ x^2+2 & 2x+1 \end{bmatrix}.\begin{bmatrix} x \\ 1 \end{bmatrix}$$

$$= \begin{bmatrix} x+3 \\ 5 \end{bmatrix}$$

$$D_3 = (u_3 - v_3.s)\ mod\ 7 = \begin{bmatrix} x^3+x+3 \\ 2x^3+5x+6 \end{bmatrix} - \begin{bmatrix} x^2 & x+6 \\ 2x^2+2 & 3x+1 \end{bmatrix}.\begin{bmatrix} x \\ 1 \end{bmatrix}$$

$$= \begin{bmatrix} 4 \\ 5 \end{bmatrix}$$

$$D_4 = (u_4 - v_4.s)\ mod\ 7 = \begin{bmatrix} x^2+5 \\ x^3+6x^2+5x \end{bmatrix} - \begin{bmatrix} x & 2 \\ x^2+4x & 3x+2x^2 \end{bmatrix}.\begin{bmatrix} x \\ 1 \end{bmatrix}$$

$$= \begin{bmatrix} 3 \\ 2x \end{bmatrix}$$

$$D_5 = (u_5 - v_5.s)\ mod\ 7 = \begin{bmatrix} 5x^2+2x+3 \\ x^3+6x^2+5x \end{bmatrix} - \begin{bmatrix} 4x+1 & x^2+x+2 \\ x^2+4x & 2x^2+3x \end{bmatrix}.\begin{bmatrix} x \\ 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 \\ 2x \end{bmatrix}$$

Selanjutnya, dari hasil masing-masing dekripsi akan dijumlahkan koefisiennya dalam modulo 7. Jika hasil penjumlahannya lebih dekat ke 0 daripada $\frac{7}{2}$, maka data yang didapatkan adalah 0. Sebaliknya, jika hasil penjumlahannya lebih dekat ke $\frac{7}{2}$ daripada ke 0, maka data yang didapatkan adalah 1.

$$m_1 = \begin{bmatrix} 2 \\ 2x+4 \end{bmatrix} = \begin{bmatrix} 2 \\ 2+4 \end{bmatrix} = \begin{bmatrix} 2 \\ 6 \end{bmatrix}$$

Karena 2 lebih dekat ke 0, maka baris pertama adalah 0. Sedangkan 6 lebih dekat ke $\frac{7}{2}$, maka baris kedua adalah 1. Jadi $m_1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

$$m_2 = \begin{bmatrix} x+3 \\ 5 \end{bmatrix} = \begin{bmatrix} 1+3 \\ 5 \end{bmatrix} = \begin{bmatrix} 4 \\ 5 \end{bmatrix}$$

Karena 4 dan 5 lebih dekat ke $\frac{7}{2}$ daripada 0, maka $m_2 = \begin{bmatrix}1\\1\end{bmatrix}$

$m_3 = \begin{bmatrix}4\\5\end{bmatrix}$

Karena 4 dan 5 lebih dekat ke $\frac{7}{2}$ daripada ke 0, maka $m_7 = \begin{bmatrix}1\\1\end{bmatrix}$

$m_4 = \begin{bmatrix}3\\2x\end{bmatrix} = \begin{bmatrix}3\\2\end{bmatrix}$

Karena 3 lebih dekat ke $\frac{7}{2}$ daripada 0, maka barus pertama adalah 1. Sedangkan 2 lebih dekat ke 0, maka baris kedua adalah 0 $m_4 = \begin{bmatrix}1\\0\end{bmatrix}$

$m_5 = \begin{bmatrix}1\\2x\end{bmatrix} = \begin{bmatrix}1\\2\end{bmatrix}$

Karena 1 dan lebih dekat ke 0 daripada ke $\frac{7}{2}$, maka $m_5 = \begin{bmatrix}0\\0\end{bmatrix}$

Dari hasil dekripsi, maka data yang diterima adalah

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

Setelah mendapatkan biner, maka dikonversi ke bilangan bulat dengan cara dimulai dari bit paling kanan. Posisi tiap angka biner dimulai dari sebelah kanan, setiap angka (bit) mempunyai nilai posisi berdasarkan pangkat dua. Jadi, nomor posisinya adalah:

Posisi : 9 8 7 6 5 4 3 2 1 0

Biner : 0 1 1 1 1 1 1 0 0 0

Posisi ke-0 artinya 2^0 (atau 1), posisi ke-1 artinya 2^1 (atau 2), dan seterusnya sampai 2^9.

Kalikan setiap bit dengan nilai posisinya, lalu jumlahkan :

$$0 \cdot 2^0 + 0 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 + 1 \cdot 2^5 + 1 \cdot 2^6 + 1 \cdot 2^7 + 1 \cdot 2^8 + 0 \cdot 2^9$$

$$= 0 + 0 + 0 + 8 + 16 + 32 + 64 + 128 + 256 + 0 = 504$$

Jadi, hasil bilangan bulatnya sudah kembali ke data awal.

Hasil dari proses dekripsi dilakukan untuk mengembalikan *chipertext* ke data awal dapat dilihat pada Lampiran 2. Pada Lampiran 2 dapat dilihat bahwa setiap *chipertext* yang diterima oleh penerima akan menghasilkan sebuah bilangan biner kemudian dikonversi ke bilangan bulat. Untuk menghasilkan data, maka harus merubah bilangan biner tersebut ke data asli. Konversi dari bilangan biner ke bilangan bulat dapat dilakukan dengan cara memulai dari bit paling kanan. Posisi tiap angka biner dimulai dari sebelah kanan, setiap angka (bit) mempunyai nilai posisi berdasarkan pangkat dua. Data asli dihitung dengan menghitung chiperteks dari v_1 dan u_1 hingga pasangan *chiperteks* paling akhir seperti v_5, u_5.

4.5 Perbandingan Data Asli dengan Data Hasil Dekripsi

Perbandingan data ini diperlukan sebelum algoritma benar-benar digunakan oleh perusahaan. Analisis terhadap hasil dekripsi bertujuan untuk mengetahui algoritma *Module Learning with Errors* (MLWE) mampu mengamankan sekaligus menjaga keutuhan data transaksi PT. Indonesia Comnet Plus Surabaya. Proses ini melibatkan perbandingan langsung antara data asli sebelum dienkripsi dengan data yang telah dilakukan proses enkripsi dan kemudian didekripsi. Tujuan utama dari perbandingan ini adalah untuk memastikan bahwa data dari hasil dekripsi identik dengan data asli. Sehingga dapat dibuktikan bahwa algoritma yang diterapkan tidak menyebabkan perubahan informasi.

Metode yang digunakan dalam proses perbandingan ini adalah dengan membandingkan nilai-nilai data secara langsung, yaitu dengan melakukan pengecekan kesamaan nilai yang didapatkan dengan data asli. Apabila seluruh hasil

dekripsi menunjukkan kesesuaian dengan persentase 100 pada data asli, maka hal ini menjadi indikator bahwa implementasi algoritma MLWE telah berhasil diterapkan dengan baik. Berikut adalah tabel perbandingan data asli dengan data yang telah didekripsi.

Tabel 4.3 Perbandingan Data

Data Dekripsi	Data Asli	Status
504	504	Sesuai
282	282	Sesuai
250	250	Sesuai
190	190	Sesuai
157	157	Sesuai
156	156	Sesuai
149	149	Sesuai
136	136	Sesuai
121	121	Sesuai
102	102	Sesuai
98	98	Sesuai
89	89	Sesuai
84	84	Sesuai
79	79	Sesuai
77	77	Sesuai
70	70	Sesuai
67	67	Sesuai
63	63	Sesuai
52	52	Sesuai
49	49	Sesuai
44	44	Sesuai
39	39	Sesuai
34	34	Sesuai
30	30	Sesuai
27	27	Sesuai
23	23	Sesuai
21	21	Sesuai
11	11	Sesuai
7	7	Sesuai
2	2	Sesuai

Berdasarkan Tabel 4.3 di atas, seluruh data cocok dengan data awal yang akan dikirimkan. Maka dapat disimpulkan bahwa skema MLWE yang diimplementasikan telah berhasil menjaga integritas dan keakuratan data transaksi.

Ini menunjukkan bahwa metode ini layak digunakan dalam lingkungan dunia nyata seperti pengamanan data transaksi pada PT. Indonesia Comnet Plus Surabaya. Dengan demikian, melalui perbandingan ini dapat disimpulkan bahwa kendala sistem kriptografi berbasis MLWE sangat bergantung pada ketepatan implementasi serta pemilihan parameter yang sesuai, agar proses enkripsi dan dekripsi dapat berjalan secara efisien tanpa mengorbankan integritas data yang dilindungi.

Hasil implementasi enkripsi dan dekripsi menggunakan skema MLWE menunjukkan bahwa data yang telah dienkripsi tidak dapat dikenali atau dibaca oleh pihak yang tidak memiliki kunci privat. Hal ini ditunjukkan dengan *ciphertext* yang bersifat acak dan tidak memiliki pola yang dapat ditebak. Selain itu, proses dekripsi berhasil mengembalikan *cipher*text menjadi data asli secara tepat, yang menandakan bahwa sistem ini memiliki keandalan tinggi. Penambahan *error* dalam proses enkripsi menjadi faktor utama yang membuat algoritma ini tahan terhadap berbagai jenis serangan (Taha & Eisenbarth, 2015). *Error* ditambahkan membuat sistem persamaan linier yang digunakan dalam enkripsi menjadi sulit untuk dipecahkan karena solusi dari persamaan menjadi kabur dan tidak dapat diperoleh secara langsung. Hal ini dapat mempersulit upaya pemulihan kunci rahasia. Oleh karena itu, implementasi MLWE terbukti mampu memberikan tingkat keamanan tinggi dalam pengamanan data transaksi, dan menjadi pilihan algoritma kriptografi yang menjanjikan.

4.6 Kajian Keislaman dengan Hasil Penelitian

Keamanan data transaksi menjadi aspek penting dalam perkembangan zaman di era digital, karena melibatkan hak-hak individu dan perusahaan atas informasi

yang bersifat pribadi. Dalam islam, menjaga privasi dan melindungi hak orang lain adalah bagian dari nilai-nilai moral yang tinggi, serta termasuk dalam bentuk amanah yang harus dijaga dengan penuh tanggung jawab. Setiap usaha untuk melindungi data dan mencegah penyalahgunaan informasi merupakan perbuatan baik yang akan membawa manusia menuju golongan kanan, yaitu golongan orang-orang yang mendapatkan keridhaan Allah SWT.

Penelitian ini menghadirkan solusi inovatif melalui implementasi metode *Module Learning with Errors* (MLWE) dalam sistem pengamanan data transaksi di PT. Indonesia Comnet Plus. Metode ini bertujuan untuk mencegah kebocoran informasi dan melindungi hak-hak semua pihak yang terlibat. Dengan penelitian ini diharapkan dapat memperkuat sistem keamanan informasi dan mencegah akses pihak yang tidak berwenang terhadap data yang dianggap penting serta dapat menciptakan rasa aman dan kepercayaan yang lebih besar dalam kegiatan transaksi digital.

Melalui penerapan metode ini, penelitian ini tidak hanya berkontribusi dalam pengembangan ilmu pengetahuan di bidang keamanan informasi, tetapi juga mencerminkan pelaksanaan nilai-nilai etika dalam islam. Penelitian ini juga mengingatkan pada tanggung jawab manusia sebagai khalifah di bumi untuk menjaga keadilan, keamanan, dan hak-hak sesama. Penggunaan metode kriptografi ini dapat menjadi sarana untuk menunaikan amanah dan menjaga hak-hak yang Allah SWT titipkan kepada manusia. Harapannya, inovasi ini dapat menjadi jalan untuk menjaga keadilan, kepercayaan, dan kehormatan sesama manusia, serta menjadi amal kebaikan yang mempererat hubungan antara manusia dan penciptanya.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang diperoleh, dapat disimpulkan bahwa implementasi skema *Module Learning with Errors* (MLWE) berhasil diterapkan untuk mengamankan data transaksi PT. Indonesia Comnet Plus Surabaya dengan baik. Data transaksi yang berupa bilangan bulat dikonversi ke bentuk biner dan berhasil dienkripsi menggunakan skema MLWE menjadi pasangan *ciphertext* yang aman. Proses enkripsi dilakukan per dua bit dengan menambahkan *noise* acak untuk meningkatkan keamanan. Selanjutnya, proses dekripsi dengan menggunakan kunci privat mampu mengembalikan *ciphertext* ke bentuk biner dan dikonversi kembali ke data asli secara akurat. Seluruh data hasil dekripsi menunjukkan kesesuaian 100% dengan data asli, sehingga membuktikan bahwa skema MLWE yang diterapkan tidak hanya mampu menjaga kerahasiaan data, tetapi juga menjamin keutuhan informasi.

Hasil penelitian juga menunjukkan bahwa representasi *ciphertext* dalam bentuk polinomial meskipun memberikan keamanan tinggi, memiliki kelemahan dari sisi efisiensi penyimpanan karena memerlukan memori yang cukup besar. Oleh karena itu, sebagai alternatif disusun program untuk penyimpanan *ciphertext* dalam bentuk non-polinomial yang lebih ringkas namun tetap aman. Alternatif ini dapat mengurangi penggunaan ruang penyimpanan tanpa mengurangi kualitas perlindungan terhadap data, karena *ciphertext* tetap tidak dapat dibaca tanpa kunci privat, dan proses dekripsi tetap mampu mengembalikan data ke bentuk semula.

Dengan demikian, skema MLWE yang diimplementasikan dalam penelitian ini terbukti layak digunakan sebagai metode kriptografi post-kuantum dalam menjaga kerahasiaan dan integritas data transaksi secara efisien dan aman.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, beberapa rekomendasi dapat diberikan untuk penelitian selanjutnya guna memperluas cakupan implementasi dan memperdalam pemahaman terkait pengamanan data transaksi menggunakan *Module Learning with Errors* (MLWE). Saran ini diharapkan dapat memberikan arahan dalam pengembangan sistem keamanan data yang lebih komprehensif dan efisien.

1. Pada penelitian ini, implementasi MLWE telah berhasil menjaga integritas data dengan tingkat keberhasilan 100%. Untuk penelitian selanjutnya, disarankan untuk menguji skema ini pada jenis data yang lebih beragam, seperti data real-time, untuk mengetahui sejauh mana performa MLWE terhadap volume data yang lebih kompleks
2. Dataset yang digunakan dalam penelitian ini terbatas pada jumlah transaksi mitra selama empat tahun terakhir. Untuk memperluas cakupan dan ketahanan sistem, penelitian ini di masa mendatang dapat mempertimbangkan penggunaan dataset dari berbagai jenis transaksi dan skenario operasional yang lebih dinamis.
3. Pada penelitian ini, pengujian dilakukan dengan satu set parameter modulus, *noise*, dan rank yang telah ditentukan. Untuk meningkatkan efisiensi, penelitian mendatang dapat mengeksplorasi variasi parameter MLWE atau

membandingkannya dengan varian *post-quantum* dari kriptografi lainnya yang bertujuan untuk mendapatkan keseimbangan terbaik antara keamanan dan kecepatan proses.

4. Dalam penelitian ini, penyimpanan data hasil enkripsi dan dekripsi masih dilakukan menggunakan media penyimpanan sederhana. Oleh karena itu, untuk penelitian selanjutnya disarankan agar dilakukan pengembangan pada sistem penyimpanan data, khususnya dalam hal manajemen basis data dan efisiensi penggunaan memori. Mengingat semakin banyak jumlah data yang dienkripsi dan disimpan, maka kebutuhan akan kapasitas memori yang besar juga akan meningkat. Oleh sebab itu, perlu dipertimbangkan penggunaan sistem manajemen basis data yang lebih optimal dan dukungan infrastruktur penyimpanan yang memadai agar mampu menangani skala data yang lebih besar secara efisien dan aman.

DAFTAR PUSTAKA

Boudgoust, K., Jeudy, C., Roux-langlois, A., Wen, W., Boudgoust, K., Jeudy, C., & Roux-langlois, A. (2023). *On the Hardness of Module Learning With Errors with Short Distributions*. *Journal of Cryptology*, *36*(1), 1–70.

Haryadi, E., & Ladjamuddin, S. M. (2017). Message Security Techniquies Using Cryptography With Vernam Chiper Algorithm. *Teknik Keamanan-Edi Haryadi Incomtech*, *6*(1), 40–47. ISSN 2337-6805.

Ibn Kathir. (2004). *Tafsir Ibnu Katsir (6.1)*. Jakarta: Pustaka Ibnu Katsir.

Kementrian Agama RI. (2024). *Qur'an Kemenag*. Lajnah Pentashihan Mushaf Al- Qur'an.

Kromodimoeljo, S. (2009). *Teori&aplikasi*. SPK IT Consulting. ISBN 978-602-96233-0-7.

Langlois, A., & Stehlé, D. (2015). Worst-case to average-case reductions for module lattices. *Designs, Codes, and Cryptography*, *75*(3), 565–599. https://doi.org/10.1007/s10623-014-9938-4

Liestyowati, D. (2020). Public Key Cryptography. *Journal of Physics: Conference Series*, *1477*(5). https://doi.org/10.1088/1742-6596/1477/5/052062

Lusiana, V., & Handikurniawati, W. (2010). Kriptografi Kunci Publik . *Dinamika Informatika*, *II*(1), 1–5.

Munanda, E., & Monalisa, S. (2021). Penerapan Algoritma Fp-Growth Pada Data Transaksi Penjualan Untuk Penentuan Tataletak. *Jurnal Ilmiah Rekayasa Dan Manajemen Sistem Informasi*, *7*(2), 173–184. http://ejournal.uin-suska.ac.id/index.php/RMSI/article/view/13253

Olva, M., Dwiputri Permatasari, R., Majid, S., Syair, P., & Suganda, A. (2021). Pemanfaatan Dasbor pada Pemantauan Data Transaksi Penjualan. *Journal of Engineering, Technology, and Applied Science*, *3*(1), 1–15. https://doi.org/10.36079/lamintang.jetas-0301.188

Pipit Muliyah, Dyah Aminatun, Sukma Septian Nasution, Tommy Hastomo, Setiana Sri Wahyuni Sitepu, T. (2020). *Journal GEEJ*, *7*(2).

Priliasari, E. (2023). Perlindungan Data Pribadi Konsumen dalam Transaksi E-Commerce menurut Peraturan Perundang-Undangan di Indonesia (Legal Protection of Consumer Personal Data in E-Commerce According To Laws dan Regulations in Indonesia). *Jurnal Rechts Vinding*, *12*(2), 261–279.

Rasiman, Rubowo, M. R., & Pramasdyahsari, A. S. (2018). Teori Ring. *Maret*, 61–79. http://eprints.upgris.ac.id/637/1/Buku Teori Ring.pdf

Sebastian, K., & Tjahyana, S. (n.d.). *Implementasi Algoritma Kriptografi Post-Quantum dalam Sistem Keamanan SSL / TLS*. 1–12.

Taha, M., & Eisenbarth, T. (2015). *Implementation attacks on post-quantum cryptographic schemes.* Worcester Polytechnic Institute.

Yusniah, Y., Putri, A., & Simatupang, A. (2022). Perkembangan Teknologi Komunikasi dan Informasi: Akar Revolusi dan Berbagai Standarnya. *Da'watuna: Journal of Communication and Islamic Broadcasting*, *3*(2), 330–337. https://doi.org/10.47467/dawatuna.v3i2.2460

LAMPIRAN

Lampiran 1 Hasil Enkripsi

Data	Chipertext
504	$(v_1,u_1)=\left(\begin{bmatrix}4x+3 & 3+x^2+2x\\ x^2+4x & 2x^2+3x+6\end{bmatrix},\begin{bmatrix}5x^2+5x+5\\ x^3+5x+6x^2+3\end{bmatrix}\right)$
	$(v_2,u_2)=\left(\begin{bmatrix}2x & x^2+x\\ x^2+2 & 2x+1\end{bmatrix},\begin{bmatrix}3x^2+2x+3\\ x^3+4x+6\end{bmatrix}\right)$
	$(v_3,u_3)=\left(\begin{bmatrix}x^2 & x+6\\ 2x^2+2 & 3x+1\end{bmatrix},\begin{bmatrix}x^3+x+3\\ 2x^3+5x+6\end{bmatrix}\right)$
	$(v_4,u_4)=\left(\begin{bmatrix}x & 2\\ x^2+4x & 3x+2x^2\end{bmatrix},\begin{bmatrix}x^2+5\\ x^3+6x^2+5x\end{bmatrix}\right)$
	$(v_5,u_5)=\left(\begin{bmatrix}4x+1 & x^2+x+2\\ x^2+4x & 2x^2+3x\end{bmatrix},\begin{bmatrix}5x^2+2x+3\\ x^3+6x^2+5x\end{bmatrix}\right)$
282	$(v_1,u_1)=\left(\begin{bmatrix}2x & x^2+x\\ x^2+3 & 2x+1\end{bmatrix},\begin{bmatrix}3x^2+2x\\ x^3+4x+6\end{bmatrix}\right)$
	$(v_2,u_2)=\left(\begin{bmatrix}4x+3 & x^2+2x+3\\ x^2+4x & 2x^2+3x+6\end{bmatrix},\begin{bmatrix}5x^2+5x+5\\ x^3+6x^2+5x\end{bmatrix}\right)$
	$(v_3,u_3)=\left(\begin{bmatrix}x & 2\\ x^2+4x & 2x^2+3x\end{bmatrix},\begin{bmatrix}x^2+2\\ x^3+6x^2+5x+3\end{bmatrix}\right)$
	$(v_4,u_4)=\left(\begin{bmatrix}2x & x^2+x\\ 2x^2+2 & 3x+2\end{bmatrix},\begin{bmatrix}3x^2+2x+4\\ 2x^3+5x+2\end{bmatrix}\right)$
	$(v_5,u_5)=\left(\begin{bmatrix}4x+1 & x^2+x+2\\ 2x^2+4 & 3x+1\end{bmatrix},\begin{bmatrix}5x^2+2x+6\\ 2x^3+5x+2\end{bmatrix}\right)$
250	$(v_1,u_1)=\left(\begin{bmatrix}4x+1 & x^2+x+2\\ x^2+4x & 2x^2+3x\end{bmatrix},\begin{bmatrix}5x^2+2x+6\\ x^3+6x^2+5x+3\end{bmatrix}\right)$
	$(v_2,u_2)=\left(\begin{bmatrix}3x & x^2+x+1\\ 2x+1 & x^2+x\end{bmatrix},\begin{bmatrix}4x^2+2x+4\\ 3x^2+2x+4\end{bmatrix}\right)$
	$(v_3,u_3)=\left(\begin{bmatrix}x^2+x+4 & 3x+3\\ 2x^2+3 & 3x+1\end{bmatrix},\begin{bmatrix}x^3+x^2+1\\ 2x^3+5x+3\end{bmatrix}\right)$
	$(v_4,u_4)=\left(\begin{bmatrix}2x+2 & x^2+2x+1\\ 2x^2+3 & 3x+1\end{bmatrix},\begin{bmatrix}3x^2+5x+6\\ 2x^3+5x+2\end{bmatrix}\right)$
190	$(v_1,u_1)=\left(\begin{bmatrix}x^2+1 & x\\ x^2+5x & 2x^2+3x+1\end{bmatrix},\begin{bmatrix}x^3+x+4\\ x^3+7x^2+5x+1\end{bmatrix}\right)$
	$(v_2,u_2)=\left(\begin{bmatrix}x^2+2x & x+3\\ 3x & x^2+x+1\end{bmatrix},\begin{bmatrix}x^3+2x^2+x+6\\ 4x^2+2x+4\end{bmatrix}\right)$
	$(v_3,u_3)=\left(\begin{bmatrix}2x^2+2 & 3x+1\\ 4x+1 & x^2+x+2\end{bmatrix},\begin{bmatrix}2x^3+5x+6\\ 5x^2+2x+5\end{bmatrix}\right)$

Data	Chipertext
	$(v_4, u_4) = \left(\begin{bmatrix} x^2+4 & 3x+2 \\ 4x+2 & 2x^2+3x+2 \end{bmatrix}, \begin{bmatrix} x^3+1 \\ 6x^2+2 \end{bmatrix}\right)$
157	$(v_1, u_1) = \left(\begin{bmatrix} 3x+1 & x^2+x+1 \\ 4x+2 & x^2+2x+3 \end{bmatrix}, \begin{bmatrix} 4x^2+2x+4 \\ 5x^2+5x+5 \end{bmatrix}\right)$
	$(v_2, u_2) = \left(\begin{bmatrix} x^2+2x+2 & x^2+3x+2 \\ x^2+2 & 2x+1 \end{bmatrix}, \begin{bmatrix} x^3+3x^2+6x+2 \\ x^3+4x+6 \end{bmatrix}\right)$
	$(v_3, u_3) = \left(\begin{bmatrix} 2x & x^2+x \\ x^2+3x+1 & x^2+2x+1 \end{bmatrix}, \begin{bmatrix} 3x^2+2x+3 \\ x^3+4x^2+3x+5 \end{bmatrix}\right)$
	$(v_4, u_4) = \left(\begin{bmatrix} 3x & x^2+x+1 \\ 2x & x^2+x+1 \end{bmatrix}, \begin{bmatrix} 4x^2+2x+1 \\ 3x^2+2x+4 \end{bmatrix}\right)$
156	$(v_1, u_1) = \left(\begin{bmatrix} x^2+5 & 3x+2 \\ 2x^2+3x & x^2+3x+1 \end{bmatrix}, \begin{bmatrix} x^3+1 \\ 2x^3+4x^2+4x+1 \end{bmatrix}\right)$
	$(v_2, u_2) = \left(\begin{bmatrix} x^2+x+2 & 2x+3 \\ 2x^2+4 & 4x+2 \end{bmatrix}, \begin{bmatrix} x^3+x^2+4x+4 \\ 2x^3+8x \end{bmatrix}\right)$
	$(v_3, u_3) = \left(\begin{bmatrix} x & 1 \\ 2x^2+5x+1 & 2x^2+4x+1 \end{bmatrix}, \begin{bmatrix} x^2+5 \\ 2x^3+6x+4 \end{bmatrix}\right)$
	$(v_4, u_4) = \left(\begin{bmatrix} 2 & x+1 \\ x^2+2x+2 & x^2+3x+2 \end{bmatrix}, \begin{bmatrix} 3x+3 \\ x^3+3x^2+6x+2 \end{bmatrix}\right)$
149	$(v_1, u_1) = \left(\begin{bmatrix} 5x+1 & 2x^2+2x+1 \\ x^2+2 & 2x+1 \end{bmatrix}, \begin{bmatrix} 4x+4 \\ x^3+4x+3 \end{bmatrix}\right)$
	$(v_2, u_2) = \left(\begin{bmatrix} x^2+2x+4 & x^2+4x+3 \\ 3x & x^2+x+1 \end{bmatrix}, \begin{bmatrix} x^3+3x^2+2x+4 \\ 4x^2+2x+5 \end{bmatrix}\right)$
	$(v_3, u_3) = \left(\begin{bmatrix} x^2+x+4 & 3x+3 \\ 2x^2+1 & 2x \end{bmatrix}, \begin{bmatrix} x^3+x^2+5 \\ 2x^3+2x+4 \end{bmatrix}\right)$
	$(v_4, u_4) = \left(\begin{bmatrix} x^2+2x+2 & 2x+3 \\ 2x+2 & x^2+2x+3 \end{bmatrix}, \begin{bmatrix} x^3+2x^2+4x+4 \\ 3x^2+5x+6 \end{bmatrix}\right)$
136	$(v_1, u_1) = \left(\begin{bmatrix} 3x+5 & x^2+3x+3 \\ 2x^2+4 & 4x+2 \end{bmatrix}, \begin{bmatrix} 4x^2+x+2 \\ 2x^3+x+4 \end{bmatrix}\right)$
	$(v_2, u_2) = \left(\begin{bmatrix} 2x+4 & x^2+3x+3 \\ 2x^2+2x & x^2+3x \end{bmatrix}, \begin{bmatrix} 3x^2+x+5 \\ 2x^3+3x^2+4x \end{bmatrix}\right)$
	$(v_3, u_3) = \left(\begin{bmatrix} 2x^2+2x & x^2+3x \\ x^2+1 & x \end{bmatrix}, \begin{bmatrix} 2x^3+3x^2+4x+3 \\ x^3+x+1 \end{bmatrix}\right)$
	$(v_4, u_4) = \left(\begin{bmatrix} 2x^2 & 2x \\ x^2+4x & x^2+2x+3 \end{bmatrix}, \begin{bmatrix} 2x^3+2x+1 \\ x^3+5x^2+3x+2 \end{bmatrix}\right)$
121	$(v_1, u_1) = \left(\begin{bmatrix} 3x+1 & x^2+x+1 \\ 2x^2+2x+4 & x^2+5x+2 \end{bmatrix}, \begin{bmatrix} 4x^2+2x+2 \\ 2x^3+3x^2+3x \end{bmatrix}\right)$
	$(v_2, u_2) = \left(\begin{bmatrix} 4x & x^2+x+3 \\ x^2+5x & 2x^2+3x+1 \end{bmatrix}, \begin{bmatrix} 5x^2+2x+6 \\ x^3+5x+4 \end{bmatrix}\right)$

Data	Chipertext
	$(v_3, u_3) = \left(\begin{bmatrix} 3x+2 & x^2+2x+2 \\ x^2+4x+1 & 2x^2+3x \end{bmatrix}, \begin{bmatrix} 4x^2+5x \\ x^3+6x^2+5x \end{bmatrix}\right)$
	$(v_4, u_4) = \left(\begin{bmatrix} 3x & x^2+x+1 \\ 4x & x^2+x+3 \end{bmatrix}, \begin{bmatrix} 4x^2+2x+1 \\ 5x^2+2x+6 \end{bmatrix}\right)$
102	$(v_1, u_1) = \left(\begin{bmatrix} 3x+3 & x^2+2x+2 \\ 2x^2 & 2x \end{bmatrix}, \begin{bmatrix} 4x^2+5x+3 \\ 2x^3+2x+4 \end{bmatrix}\right)$
	$(v_2, u_2) = \left(\begin{bmatrix} x^2+4 & 3x+3 \\ 4x & x^2+x+2 \end{bmatrix}, \begin{bmatrix} x^3+1 \\ 5x^2+2x+2 \end{bmatrix}\right)$
	$(v_3, u_3) = \left(\begin{bmatrix} 4x+2 & x^2+2x+3 \\ x^2+1 & x \end{bmatrix}, \begin{bmatrix} 5x^2+5x+4 \\ x^3+x+4 \end{bmatrix}\right)$
	$(v_4, u_4) = \left(\begin{bmatrix} 2x^2 & 2x \\ x^2+2x+4 & 3x+5 \end{bmatrix}, \begin{bmatrix} 2x^3+2x+3 \\ x^3+2x^2 \end{bmatrix}\right)$
98	$(v_1, u_1) = \left(\begin{bmatrix} x+5 & 2x+3 \\ x^2+5x & 2x^2+3x+1 \end{bmatrix}, \begin{bmatrix} x^2+6x+6 \\ x^3+5x+4 \end{bmatrix}\right)$
	$(v_2, u_2) = \left(\begin{bmatrix} 4x & x^2+x+3 \\ x^2+4x & 2x^2+3x \end{bmatrix}, \begin{bmatrix} 5x^2+2x+6 \\ x^3+6x^2+5x \end{bmatrix}\right)$
	$(v_3, u_3) = \left(\begin{bmatrix} x^2 & x \\ 5x+1 & 2x^2+2x+1 \end{bmatrix}, \begin{bmatrix} x^3+x+1 \\ 4x+1 \end{bmatrix}\right)$
	$(v_4, u_4) = \left(\begin{bmatrix} x^2+2x & x+2 \\ x^2 & x+1 \end{bmatrix}, \begin{bmatrix} x^3+2x^2+x+5 \\ x^3+x+1 \end{bmatrix}\right)$
89	$(v_1, u_1) = \left(\begin{bmatrix} 2x^2+3 & 3x+1 \\ 2x & 2 \end{bmatrix}, \begin{bmatrix} 2x^3+5x+3 \\ 2x^2+5 \end{bmatrix}\right)$
	$(v_2, u_2) = \left(\begin{bmatrix} x^2+x & x+2 \\ 2x & x^2+x \end{bmatrix}, \begin{bmatrix} x^3+x^2+x+2 \\ 3x^2+2x+3 \end{bmatrix}\right)$
	$(v_3, u_3) = \left(\begin{bmatrix} x^2+2x & x+2 \\ 3x+1 & x^2+x+1 \end{bmatrix}, \begin{bmatrix} x^3+2x^2+x+6 \\ 4x^2+2x+1 \end{bmatrix}\right)$
	$(v_4, u_4) = \left(\begin{bmatrix} 4x & x^2+x+2 \\ x^2+4x & 2x^2+3x+1 \end{bmatrix}, \begin{bmatrix} 5x^2+2x+2 \\ x^3+6x^2+5x+4 \end{bmatrix}\right)$
84	$(v_1, u_1) = \left(\begin{bmatrix} x^2+3 & 2x+1 \\ x^2+3x+4 & x^2+4x+3 \end{bmatrix}, \begin{bmatrix} x^3+4x+3 \\ x^3+4x^2+2x+1 \end{bmatrix}\right)$
	$(v_2, u_2) = \left(\begin{bmatrix} x^2+5x & 2x^2+3x+2 \\ x^2+4 & 3x+2 \end{bmatrix}, \begin{bmatrix} x^3+5x+2 \\ x^3 \end{bmatrix}\right)$
	$(v_3, u_3) = \left(\begin{bmatrix} x^2+4x & x^2+2x+2 \\ x^2+5 & 3x+2 \end{bmatrix}, \begin{bmatrix} x^3+5x^2+3x+3 \\ x^3 \end{bmatrix}\right)$
	$(v_4, u_4) = \left(\begin{bmatrix} x^2+3x & x^2+2x+1 \\ x^2 & x+1 \end{bmatrix}, \begin{bmatrix} x^3+4x^2+3x+1 \\ x^3+x+1 \end{bmatrix}\right)$
	$(v_1, u_1) = \left(\begin{bmatrix} 3x+1 & x^2+x+1 \\ 2x^2+4 & 4x+2 \end{bmatrix}, \begin{bmatrix} 4x^2+2x+1 \\ 2x^3+x+1 \end{bmatrix}\right)$

Data	Chipertext
79	$(v_2, u_2) = \left(\begin{bmatrix} x^2+4x & 2x^2+3x+1 \\ x^2+2 & 2x+1 \end{bmatrix}, \begin{bmatrix} x^3+6x^2+5x \\ x^3+4x+3 \end{bmatrix}\right)$
	$(v_3, u_3) = \left(\begin{bmatrix} 2x^2+2x & x^2+3x \\ 4x+1 & x^2+x+2 \end{bmatrix}, \begin{bmatrix} 2x^3+3x^2+4x+3 \\ 5x^2+2x+6 \end{bmatrix}\right)$
	$(v_4, u_4) = \left(\begin{bmatrix} 3x & x^2+x+1 \\ 5x & 2x^2+2x+2 \end{bmatrix}, \begin{bmatrix} 4x^2+2x+4 \\ 4x+5 \end{bmatrix}\right)$
77	$(v_1, u_1) = \left(\begin{bmatrix} x^2+3 & 2x+1 \\ x^2+x & x+1 \end{bmatrix}, \begin{bmatrix} x^3+4x+2 \\ x^3+x^2+x+5 \end{bmatrix}\right)$
	$(v_2, u_2) = \left(\begin{bmatrix} x^2+3x & x^2+2x+2 \\ 3x & x^2+x+1 \end{bmatrix}, \begin{bmatrix} x^3+4x^2+3x+1 \\ 4x^2+2x+2 \end{bmatrix}\right)$
	$(v_3, u_3) = \left(\begin{bmatrix} 3x & x^2+x+1 \\ 2x^2+2x+1 & x^2+3x \end{bmatrix}, \begin{bmatrix} 4x^2+2x+4 \\ 2x^3+3x^2+4x+4 \end{bmatrix}\right)$
	$(v_4, u_4) = \left(\begin{bmatrix} x^2+2 & 2x+1 \\ 4x+2 & 2x^2+3x+2 \end{bmatrix}, \begin{bmatrix} x^3+4x+2 \\ 6x^2+6 \end{bmatrix}\right)$
70	$(v_1, u_1) = \left(\begin{bmatrix} x^2+2x+3 & 2x+3 \\ x^2 & x \end{bmatrix}, \begin{bmatrix} x^3+2x^2+4x+5 \\ x^3+x+3 \end{bmatrix}\right)$
	$(v_2, u_2) = \left(\begin{bmatrix} x^2+4x & 2x^2+3x+1 \\ x^2+2 & 2x+1 \end{bmatrix}, \begin{bmatrix} x^3+6x^2+5x+1 \\ x^3+4x+2 \end{bmatrix}\right)$
	$(v_3, u_3) = \left(\begin{bmatrix} x^2+x & x+1 \\ x^2+x+3 & 2x+2 \end{bmatrix}, \begin{bmatrix} x^3+x^2+x+2 \\ x^3+x^2+4x+6 \end{bmatrix}\right)$
	$(v_4, u_4) = \left(\begin{bmatrix} 2x+2 & x^2+2x+1 \\ x^2+x+2 & 2x+3 \end{bmatrix}, \begin{bmatrix} 3x^2+5x+6 \\ x^3+x^2+4x+3 \end{bmatrix}\right)$
67	$(v_1, u_1) = \left(\begin{bmatrix} 3x+1 & x^2+x+1 \\ 4x & x^2+x+2 \end{bmatrix}, \begin{bmatrix} 4x^2+2x+1 \\ 5x^2+2x+6 \end{bmatrix}\right)$
	$(v_2, u_2) = \left(\begin{bmatrix} x^2+2 & 2x+2 \\ 2x^2+2 & 3x+1 \end{bmatrix}, \begin{bmatrix} x^3+4x+2 \\ 2x^3+5x+3 \end{bmatrix}\right)$
	$(v_3, u_3) = \left(\begin{bmatrix} x^2+4x & 2x^2+3x \\ x+1 & 1 \end{bmatrix}, \begin{bmatrix} x^3+6x^2+5x \\ x^2+2 \end{bmatrix}\right)$
	$(v_4, u_4) = \left(\begin{bmatrix} 4x+2 & x^2+2x+3 \\ x^2+4x & 2x^2+3x+2 \end{bmatrix}, \begin{bmatrix} 5x^2+5x \\ x^3+6x^2+5x+4 \end{bmatrix}\right)$
63	$(v_1, u_1) = \left(\begin{bmatrix} x^2+2x+3 & x^2+3x+1 \\ x^2+x & x+1 \end{bmatrix}, \begin{bmatrix} x^3+3x^2+6x+5 \\ x^3+x^2+x+5 \end{bmatrix}\right)$
	$(v_2, u_2) = \left(\begin{bmatrix} x^2+x+2 & 2x+3 \\ x^2+x & x+1 \end{bmatrix}, \begin{bmatrix} x^3+x^2+4x+6 \\ x^3+x^2+x+5 \end{bmatrix}\right)$
	$(v_3, u_3) = \left(\begin{bmatrix} 2x^2+4 & 4x+2 \\ 2x^2+3 & 3x+1 \end{bmatrix}, \begin{bmatrix} 2x^3+x \\ 2x^3+5x+6 \end{bmatrix}\right)$
	$(v_1, u_1) = \left(\begin{bmatrix} x^2+2x+5 & 3x+4 \\ x^2+2x & x+2 \end{bmatrix}, \begin{bmatrix} x^3+2x^2+3 \\ x^3+2x^2+x+5 \end{bmatrix}\right)$

Data	Chipertext
52	$(v_2, u_2) = \left(\begin{bmatrix} x^2+x & x+2 \\ x^2 & x \end{bmatrix}, \begin{bmatrix} x^3+x^2+x+2 \\ x^3+x+3 \end{bmatrix}\right)$
	$(v_3, u_3) = \left(\begin{bmatrix} 2x^2+2 & 3x+1 \\ x^2+2x+3 & 2x+3 \end{bmatrix}, \begin{bmatrix} 2x^3+5x+3 \\ x^3+2x^2+4x+4 \end{bmatrix}\right)$
49	$(v_1, u_1) = \left(\begin{bmatrix} 2x^2+2x+1 & x^2+3x \\ x^2+2 & 2x+1 \end{bmatrix}, \begin{bmatrix} 2x^3+3x^2+4x+3 \\ x^3+4x+6 \end{bmatrix}\right)$
	$(v_2, u_2) = \left(\begin{bmatrix} x^2 & x+1 \\ 2x^2 & 2x \end{bmatrix}, \begin{bmatrix} x^3+x+1 \\ 2x^3+2x \end{bmatrix}\right)$
	$(v_3, u_3) = \left(\begin{bmatrix} 2x^2+2x & x^2+3x \\ x^2+3 & 2x+1 \end{bmatrix}, \begin{bmatrix} 2x^3+3x^2+4x+1 \\ x^3+4x+5 \end{bmatrix}\right)$
44	$(v_1, u_1) = \left(\begin{bmatrix} x^2+3x+5 & x^2+4x+3 \\ x^2+2 & 2x+1 \end{bmatrix}, \begin{bmatrix} x^3+4x^2+2x+1 \\ x^3+4x+3 \end{bmatrix}\right)$
	$(v_2, u_2) = \left(\begin{bmatrix} x^2+4x & x^2+2x+3 \\ x^2+x+2 & 2x+2 \end{bmatrix}, \begin{bmatrix} x^3+5x^2+3x+5 \\ x^3+x^2+4x \end{bmatrix}\right)$
	$(v_3, u_3) = \left(\begin{bmatrix} x^2+2 & 2x+1 \\ x^2+2x+3 & x^2+3x+1 \end{bmatrix}, \begin{bmatrix} x^3+4x+2 \\ x^3+3x^2+6x+3 \end{bmatrix}\right)$
39	$(v_1, u_1) = \left(\begin{bmatrix} 3x+1 & x^2+x+1 \\ 3x+2 & x^2+2x+2 \end{bmatrix}, \begin{bmatrix} 4x^2+2x+5 \\ 4x^2+5x+3 \end{bmatrix}\right)$
	$(v_2, u_2) = \left(\begin{bmatrix} x^2+4x & 2x^2+3x+1 \\ x^2+2 & 2x+1 \end{bmatrix}, \begin{bmatrix} x^3+6x^2+5x \\ x^3+4x+6 \end{bmatrix}\right)$
	$(v_3, u_3) = \left(\begin{bmatrix} 2x^2+2 & 3x+1 \\ x^2+5 & 3x+2 \end{bmatrix}, \begin{bmatrix} 2x^3+5x+5 \\ x^3+1 \end{bmatrix}\right)$
34	$(v_1, u_1) = \left(\begin{bmatrix} x^2+4x+1 & 2x^2+3x \\ 3x & x^2+x+1 \end{bmatrix}, \begin{bmatrix} x^3+6x^2+5x+4 \\ 4x^2+2x+1 \end{bmatrix}\right)$
	$(v_2, u_2) = \left(\begin{bmatrix} x^2+4 & 3x+2 \\ x^2+x+5 & 3x+3 \end{bmatrix}, \begin{bmatrix} x^3+4 \\ x^3+x^2+6 \end{bmatrix}\right)$
	$(v_3, u_3) = \left(\begin{bmatrix} 2x^2+2x & x^2+3x \\ 4x+3 & x^2+2x+3 \end{bmatrix}, \begin{bmatrix} 2x^3+3x^2+4x+4 \\ 5x^2+5x+4 \end{bmatrix}\right)$
30	$(v_1, u_1) = \left(\begin{bmatrix} x^2+5 & 3x+2 \\ 2x^2+4 & 4x+2 \end{bmatrix}, \begin{bmatrix} x^3+5 \\ 2x^3+x \end{bmatrix}\right)$
	$(v_2, u_2) = \left(\begin{bmatrix} 2x & x^2+x+1 \\ 3x+4 & x^2+3x+3 \end{bmatrix}, \begin{bmatrix} 3x^2+2x+4 \\ 4x^2+x+1 \end{bmatrix}\right)$
	$(v_3, u_3) = \left(\begin{bmatrix} x^2+2x+2 & 2x+3 \\ 2x+3 & x+3 \end{bmatrix}, \begin{bmatrix} x^3+2x^2+4x \\ 2x^2+3x+5 \end{bmatrix}\right)$
27	$(v_1, u_1) = \left(\begin{bmatrix} x^2+2x+5 & 3x+4 \\ 4x & x^2+x+2 \end{bmatrix}, \begin{bmatrix} x^3+2x^2+6 \\ 5x^2+2x+6 \end{bmatrix}\right)$
	$(v_2, u_2) = \left(\begin{bmatrix} x^2+4 & 3x+3 \\ 2x & x^2+x \end{bmatrix}, \begin{bmatrix} x^3 \\ 3x^2+2x+1 \end{bmatrix}\right)$

Data	Chipertext
	$(v_3, u_3) = \left(\begin{bmatrix} 4x & 2x^2+2x \\ 2x+5 & x^2+3x+2 \end{bmatrix}, \begin{bmatrix} 6x^2+4x+3 \\ 3x^2+x+1 \end{bmatrix}\right)$
23	$(v_1, u_1) = \left(\begin{bmatrix} x^2+3 & 2x+1 \\ 2x^2+4 & 4x+2 \end{bmatrix}, \begin{bmatrix} x^3+4x+3 \\ 2x^3+x \end{bmatrix}\right)$
	$(v_2, u_2) = \left(\begin{bmatrix} x^2+3x & x^2+2x+2 \\ x^2+2x+2 & 2x+3 \end{bmatrix}, \begin{bmatrix} x^3+4x^2+3x+2 \\ x^3+2x^2+4x \end{bmatrix}\right)$
	$(v_3, u_3) = \left(\begin{bmatrix} 3x & x^2+x+1 \\ 2x^2+2x+1 & x^2+3x \end{bmatrix}, \begin{bmatrix} 4x^2+2x+5 \\ 2x^3+3x^2+4x+3 \end{bmatrix}\right)$
21	$(v_1, u_1) = \left(\begin{bmatrix} x^2+4x+1 & 2x^2+3x \\ x^2+4 & 3x+2 \end{bmatrix}, \begin{bmatrix} x^3+6x^2+5x \\ x^3+1 \end{bmatrix}\right)$
	$(v_2, u_2) = \left(\begin{bmatrix} 3x & x^2+x+2 \\ 3x+4 & x^2+3x+3 \end{bmatrix}, \begin{bmatrix} 4x^2+2x+1 \\ 4x^2+x+2 \end{bmatrix}\right)$
	$(v_3, u_3) = \left(\begin{bmatrix} x^2+4x & 2x^2+3x \\ 4x+1 & 2x^2+2x \end{bmatrix}, \begin{bmatrix} x^3+6x^2+5x \\ 6x^2+4x+4 \end{bmatrix}\right)$
11	$(v_1, u_1) = \left(\begin{bmatrix} x^2+4x+1 & 2x^2+3x \\ 3x+2 & x^2+2x+2 \end{bmatrix}, \begin{bmatrix} x^3+6x^2+5x+4 \\ 4x^2+5x+3 \end{bmatrix}\right)$
	$(v_2, u_2) = \left(\begin{bmatrix} x^2+2x+2 & 2x+3 \\ x^2+4x+3 & x^2+3x+3 \end{bmatrix}, \begin{bmatrix} x^3+2x^2+4x+1 \\ x^3+5x^2+6x \end{bmatrix}\right)$
7	$(v_1, u_1) = \left(\begin{bmatrix} x^2+4x+1 & x^2+2x+2 \\ 2x+4 & x^2+3x+2 \end{bmatrix}, \begin{bmatrix} x^3+5x^2+3x+2 \\ 3x^2+x+1 \end{bmatrix}\right)$
	$(v_2, u_2) = \left(\begin{bmatrix} x^2+2x & x+2 \\ x^2+2x+5 & 3x+4 \end{bmatrix}, \begin{bmatrix} x^3+2x^2+x+5 \\ x^3+2x^2+3 \end{bmatrix}\right)$
2	$(v_1, u_1) = \left(\begin{bmatrix} x^2+3x+5 & x^2+4x+3 \\ x^2+x+2 & 2x+2 \end{bmatrix}, \begin{bmatrix} x^3+4x^2+2x+2 \\ x^3+x^2+4x+3 \end{bmatrix}\right)$

Lampiran 2 *Ciphertext* setelah didekripsi

Chipertext	Hasil	Data
$(v_1, u_1) = \left(\begin{bmatrix} 4x+3 & 3+x^2+2x \\ x^2+4x & 2x^2+3x+6 \end{bmatrix}, \begin{bmatrix} 5x^2+5x+5 \\ x^3+5x+6x^2+3 \end{bmatrix}\right)$	[0,1]	504
$(v_2, u_2) = \left(\begin{bmatrix} 2x & x^2+x \\ x^2+2 & 2x+1 \end{bmatrix}, \begin{bmatrix} 3x^2+2x+3 \\ x^3+4x+6 \end{bmatrix}\right)$	[1,1]	
$(v_3, u_3) = \left(\begin{bmatrix} x^2 & x+6 \\ 2x^2+2 & 3x+1 \end{bmatrix}, \begin{bmatrix} x^3+x+3 \\ 2x^3+5x+6 \end{bmatrix}\right)$	[1,1]	
$(v_4, u_4) = \left(\begin{bmatrix} x & 2 \\ x^2+4x & 3x+2x^2 \end{bmatrix}, \begin{bmatrix} x^2+5 \\ x^3+6x^2+5x \end{bmatrix}\right)$	[1,0]	
$(v_5, u_5) = \left(\begin{bmatrix} 4x+1 & x^2+x+2 \\ x^2+4x & 2x^2+3x \end{bmatrix}, \begin{bmatrix} 5x^2+2x+3 \\ x^3+6x^2+5x \end{bmatrix}\right)$	[0,0]	
$(v_1, u_1) = \left(\begin{bmatrix} 2x & x^2+x \\ x^2+3 & 2x+1 \end{bmatrix}, \begin{bmatrix} 3x^2+2x \\ x^3+4x+6 \end{bmatrix}\right)$	[0,1]	282
$(v_2, u_2) = \left(\begin{bmatrix} 4x+3 & x^2+2x+3 \\ x^2+4x & 2x^2+3x+6 \end{bmatrix}, \begin{bmatrix} 5x^2+5x+5 \\ x^3+6x^2+5x \end{bmatrix}\right)$	[0,0]	
$(v_3, u_3) = \left(\begin{bmatrix} x & 2 \\ x^2+4x & 2x^2+3x \end{bmatrix}, \begin{bmatrix} x^2+2 \\ x^3+6x^2+5x+3 \end{bmatrix}\right)$	[0,1]	
$(v_4, u_4) = \left(\begin{bmatrix} 2x & x^2+x \\ 2x^2+2 & 3x+2 \end{bmatrix}, \begin{bmatrix} 3x^2+2x+4 \\ 2x^3+5x+2 \end{bmatrix}\right)$	[1,0]	
$(v_5, u_5) = \left(\begin{bmatrix} 4x+1 & x^2+x+2 \\ 2x^2+4 & 3x+1 \end{bmatrix}, \begin{bmatrix} 5x^2+2x+6 \\ 2x^3+5x+2 \end{bmatrix}\right)$	[1,0]	
$(v_1, u_1) = \left(\begin{bmatrix} 4x+1 & x^2+x+2 \\ x^2+4x & 2x^2+3x \end{bmatrix}, \begin{bmatrix} 5x^2+2x+6 \\ x^3+6x^2+5x+3 \end{bmatrix}\right)$	[1,1]	250
$(v_2, u_2) = \left(\begin{bmatrix} 3x & x^2+x+1 \\ 2x+1 & x^2+x \end{bmatrix}, \begin{bmatrix} 4x^2+2x+4 \\ 3x^2+2x+4 \end{bmatrix}\right)$	[1,1]	
$(v_3, u_3) = \left(\begin{bmatrix} x^2+x+4 & 3x+3 \\ 2x^2+3 & 3x+1 \end{bmatrix}, \begin{bmatrix} x^3+x^2+1 \\ 2x^3+5x+3 \end{bmatrix}\right)$	[1,0]	
$(v_4, u_4) = \left(\begin{bmatrix} 2x+2 & x^2+2x+1 \\ 2x^2+3 & 3x+1 \end{bmatrix}, \begin{bmatrix} 3x^2+5x+6 \\ 2x^3+5x+2 \end{bmatrix}\right)$	[1,0]	
$(v_1, u_1) = \left(\begin{bmatrix} x^2+1 & x \\ x^2+5x & 2x^2+3x+1 \end{bmatrix}, \begin{bmatrix} x^3+x+4 \\ x^3+7x^2+5x+1 \end{bmatrix}\right)$	[1,0]	190
$(v_2, u_2) = \left(\begin{bmatrix} x^2+2x & x+3 \\ 3x & x^2+x+1 \end{bmatrix}, \begin{bmatrix} x^3+2x^2+x+6 \\ 4x^2+2x+4 \end{bmatrix}\right)$	[1,1]	
$(v_3, u_3) = \left(\begin{bmatrix} 2x^2+2 & 3x+1 \\ 4x+1 & x^2+x+2 \end{bmatrix}, \begin{bmatrix} 2x^3+5x+6 \\ 5x^2+2x+5 \end{bmatrix}\right)$	[1,1]	
$(v_4, u_4) = \left(\begin{bmatrix} x^2+4 & 3x+2 \\ 4x+2 & 2x^2+3x+2 \end{bmatrix}, \begin{bmatrix} x^3+1 \\ 6x^2+2 \end{bmatrix}\right)$	[1,0]	

Chipertext	Hasil	Data
$(v_1, u_1) = \left(\begin{bmatrix} 3x+1 & x^2+x+1 \\ 4x+2 & x^2+2x+3 \end{bmatrix}, \begin{bmatrix} 4x^2+2x+4 \\ 5x^2+5x+5 \end{bmatrix}\right)$	[1,0]	157
$(v_2, u_2) = \left(\begin{bmatrix} x^2+2x+2 & x^2+3x+2 \\ x^2+2 & 2x+1 \end{bmatrix}, \begin{bmatrix} x^3+3x^2+6x+2 \\ x^3+4x+6 \end{bmatrix}\right)$	[0,1]	
$(v_3, u_3) = \left(\begin{bmatrix} 2x & x^2+x \\ x^2+3x+1 & x^2+2x+1 \end{bmatrix}, \begin{bmatrix} 3x^2+2x+3 \\ x^3+4x^2+3x+5 \end{bmatrix}\right)$	[1,1]	
$(v_4, u_4) = \left(\begin{bmatrix} 3x & x^2+x+1 \\ 2x & x^2+x+1 \end{bmatrix}, \begin{bmatrix} 4x^2+2x+1 \\ 3x^2+2x+4 \end{bmatrix}\right)$	[0,1]	
$(v_1, u_1) = \left(\begin{bmatrix} x^2+5 & 3x+2 \\ 2x^2+3x & x^2+3x+1 \end{bmatrix}, \begin{bmatrix} x^3+1 \\ 2x^3+4x^2+4x+1 \end{bmatrix}\right)$	[1,0]	156
$(v_2, u_2) = \left(\begin{bmatrix} x^2+x+2 & 2x+3 \\ 2x^2+4 & 4x+2 \end{bmatrix}, \begin{bmatrix} x^3+x^2+4x+4 \\ 2x^3+8x \end{bmatrix}\right)$	[0,1]	
$(v_3, u_3) = \left(\begin{bmatrix} x & 1 \\ 2x^2+5x+1 & 2x^2+4x+1 \end{bmatrix}, \begin{bmatrix} x^2+5 \\ 2x^3+6x+4 \end{bmatrix}\right)$	[1,1]	
$(v_4, u_4) = \left(\begin{bmatrix} 2 & x+1 \\ x^2+2x+2 & x^2+3x+2 \end{bmatrix}, \begin{bmatrix} 3x+3 \\ x^3+3x^2+6x+2 \end{bmatrix}\right)$	[0,0]	
$(v_1, u_1) = \left(\begin{bmatrix} 5x+1 & 2x^2+2x+1 \\ x^2+2 & 2x+1 \end{bmatrix}, \begin{bmatrix} 4x+4 \\ x^3+4x+3 \end{bmatrix}\right)$	[1,0]	149
$(v_2, u_2) = \left(\begin{bmatrix} x^2+2x+4 & x^2+4x+3 \\ 3x & x^2+x+1 \end{bmatrix}, \begin{bmatrix} x^3+3x^2+2x+4 \\ 4x^2+2x+5 \end{bmatrix}\right)$	[0,1]	
$(v_3, u_3) = \left(\begin{bmatrix} x^2+x+4 & 3x+3 \\ 2x^2+1 & 2x \end{bmatrix}, \begin{bmatrix} x^3+x^2+5 \\ 2x^3+2x+4 \end{bmatrix}\right)$	[0,1]	
$(v_4, u_4) = \left(\begin{bmatrix} x^2+2x+2 & 2x+3 \\ 2x+2 & x^2+2x+3 \end{bmatrix}, \begin{bmatrix} x^3+2x^2+4x+4 \\ 3x^2+5x+6 \end{bmatrix}\right)$	[0,1]	
$(v_1, u_1) = \left(\begin{bmatrix} 3x+5 & x^2+3x+3 \\ 2x^2+4 & 4x+2 \end{bmatrix}, \begin{bmatrix} 4x^2+x+2 \\ 2x^3+x+4 \end{bmatrix}\right)$	[1,0]	136
$(v_2, u_2) = \left(\begin{bmatrix} 2x+4 & x^2+3x+3 \\ 2x^2+2x & x^2+3x \end{bmatrix}, \begin{bmatrix} 3x^2+x+5 \\ 2x^3+3x^2+4x \end{bmatrix}\right)$	[0,0]	
$(v_3, u_3) = \left(\begin{bmatrix} 2x^2+2x & x^2+3x \\ x^2+1 & x \end{bmatrix}, \begin{bmatrix} 2x^3+3x^2+4x+3 \\ x^3+x+1 \end{bmatrix}\right)$	[1,0]	
$(v_4, u_4) = \left(\begin{bmatrix} 2x^2 & 2x \\ x^2+4x & x^2+2x+3 \end{bmatrix}, \begin{bmatrix} 2x^3+2x+1 \\ x^3+5x^2+3x+2 \end{bmatrix}\right)$	[0,0]	
$(v_1, u_1) = \left(\begin{bmatrix} 3x+1 & x^2+x+1 \\ 2x^2+2x+4 & x^2+5x+2 \end{bmatrix}, \begin{bmatrix} 4x^2+2x+2 \\ 2x^3+3x^2+3x \end{bmatrix}\right)$	[0,1]	121
$(v_2, u_2) = \left(\begin{bmatrix} 4x & x^2+x+3 \\ x^2+5x & 2x^2+3x+1 \end{bmatrix}, \begin{bmatrix} 5x^2+2x+6 \\ x^3+5x+4 \end{bmatrix}\right)$	[1,1]	
$(v_3, u_3) = \left(\begin{bmatrix} 3x+2 & x^2+2x+2 \\ x^2+4x+1 & 2x^2+3x \end{bmatrix}, \begin{bmatrix} 4x^2+5x \\ x^3+6x^2+5x \end{bmatrix}\right)$	[1,0]	

Chipertext	Hasil	Data
$(v_4, u_4) = \left(\begin{bmatrix} 3x & x^2+x+1 \\ 4x & x^2+x+3 \end{bmatrix}, \begin{bmatrix} 4x^2+2x+1 \\ 5x^2+2x+6 \end{bmatrix}\right)$	[0,1]	
$(v_1, u_1) = \left(\begin{bmatrix} 3x+3 & x^2+2x+2 \\ 2x^2 & 2x \end{bmatrix}, \begin{bmatrix} 4x^2+5x+3 \\ 2x^3+2x+4 \end{bmatrix}\right)$	[0,1]	102
$(v_2, u_2) = \left(\begin{bmatrix} x^2+4 & 3x+3 \\ 4x & x^2+x+2 \end{bmatrix}, \begin{bmatrix} x^3+1 \\ 5x^2+2x+2 \end{bmatrix}\right)$	[1,0]	
$(v_3, u_3) = \left(\begin{bmatrix} 4x+2 & x^2+2x+3 \\ x^2+1 & x \end{bmatrix}, \begin{bmatrix} 5x^2+5x+4 \\ x^3+x+4 \end{bmatrix}\right)$	[0,1]	
$(v_4, u_4) = \left(\begin{bmatrix} 2x^2 & 2x \\ x^2+2x+4 & 3x+5 \end{bmatrix}, \begin{bmatrix} 2x^3+2x+3 \\ x^3+2x^2 \end{bmatrix}\right)$	[1,0]	
$(v_1, u_1) = \left(\begin{bmatrix} x+5 & 2x+3 \\ x^2+5x & 2x^2+3x+1 \end{bmatrix}, \begin{bmatrix} x^2+6x+6 \\ x^3+5x+4 \end{bmatrix}\right)$	[0,1]	98
$(v_2, u_2) = \left(\begin{bmatrix} 4x & x^2+x+3 \\ x^2+4x & 2x^2+3x \end{bmatrix}, \begin{bmatrix} 5x^2+2x+6 \\ x^3+6x^2+5x \end{bmatrix}\right)$	[1,0]	
$(v_3, u_3) = \left(\begin{bmatrix} x^2 & x \\ 5x+1 & 2x^2+2x+1 \end{bmatrix}, \begin{bmatrix} x^3+x+1 \\ 4x+1 \end{bmatrix}\right)$	[0,0]	
$(v_4, u_4) = \left(\begin{bmatrix} x^2+2x & x+2 \\ x^2 & x+1 \end{bmatrix}, \begin{bmatrix} x^3+2x^2+x+5 \\ x^3+x+1 \end{bmatrix}\right)$	[1,0]	
$(v_1, u_1) = \left(\begin{bmatrix} 2x^2+3 & 3x+1 \\ 2x & 2 \end{bmatrix}, \begin{bmatrix} 2x^3+5x+3 \\ 2x^2+5 \end{bmatrix}\right)$	[0,1]	89
$(v_2, u_2) = \left(\begin{bmatrix} x^2+x & x+2 \\ 2x & x^2+x \end{bmatrix}, \begin{bmatrix} x^3+x^2+x+2 \\ 3x^2+2x+3 \end{bmatrix}\right)$	[0,1]	
$(v_3, u_3) = \left(\begin{bmatrix} x^2+2x & x+2 \\ 3x+1 & x^2+x+1 \end{bmatrix}, \begin{bmatrix} x^3+2x^2+x+6 \\ 4x^2+2x+1 \end{bmatrix}\right)$	[1,0]	
$(v_4, u_4) = \left(\begin{bmatrix} 4x & x^2+x+2 \\ x^2+4x & 2x^2+3x+1 \end{bmatrix}, \begin{bmatrix} 5x^2+2x+2 \\ x^3+6x^2+5x+4 \end{bmatrix}\right)$	[0,1]	
$(v_1, u_1) = \left(\begin{bmatrix} x^2+3 & 2x+1 \\ x^2+3x+4 & x^2+4x+3 \end{bmatrix}, \begin{bmatrix} x^3+4x+3 \\ x^3+4x^2+2x+1 \end{bmatrix}\right)$	[0,1]	84
$(v_2, u_2) = \left(\begin{bmatrix} x^2+5x & 2x^2+3x+2 \\ x^2+4 & 3x+2 \end{bmatrix}, \begin{bmatrix} x^3+5x+2 \\ x^3 \end{bmatrix}\right)$	[0,1]	
$(v_3, u_3) = \left(\begin{bmatrix} x^2+4x & x^2+2x+2 \\ x^2+5 & 3x+2 \end{bmatrix}, \begin{bmatrix} x^3+5x^2+3x+3 \\ x^3 \end{bmatrix}\right)$	[0,1]	
$(v_4, u_4) = \left(\begin{bmatrix} x^2+3x & x^2+2x+1 \\ x^2 & x+1 \end{bmatrix}, \begin{bmatrix} x^3+4x^2+3x+1 \\ x^3+x+1 \end{bmatrix}\right)$	[0,0]	
$(v_1, u_1) = \left(\begin{bmatrix} 3x+1 & x^2+x+1 \\ 2x^2+4 & 4x+2 \end{bmatrix}, \begin{bmatrix} 4x^2+2x+1 \\ 2x^3+x+1 \end{bmatrix}\right)$	[0,1]	79
$(v_2, u_2) = \left(\begin{bmatrix} x^2+4x & 2x^2+3x+1 \\ x^2+2 & 2x+1 \end{bmatrix}, \begin{bmatrix} x^3+6x^2+5x \\ x^3+4x+3 \end{bmatrix}\right)$	[0,0]	

Chipertext	Hasil	Data
$(v_3, u_3) = \left(\begin{bmatrix} 2x^2+2x & x^2+3x \\ 4x+1 & x^2+x+2 \end{bmatrix}, \begin{bmatrix} 2x^3+3x^2+4x+3 \\ 5x^2+2x+6 \end{bmatrix}\right)$	[1,1]	
$(v_4, u_4) = \left(\begin{bmatrix} 3x & x^2+x+1 \\ 5x & 2x^2+2x+2 \end{bmatrix}, \begin{bmatrix} 4x^2+2x+4 \\ 4x+5 \end{bmatrix}\right)$	[1,1]	
$(v_1, u_1) = \left(\begin{bmatrix} x^2+3 & 2x+1 \\ x^2+x & x+1 \end{bmatrix}, \begin{bmatrix} x^3+4x+2 \\ x^3+x^2+x+5 \end{bmatrix}\right)$	[0,1]	77
$(v_2, u_2) = \left(\begin{bmatrix} x^2+3x & x^2+2x+2 \\ 3x & x^2+x+1 \end{bmatrix}, \begin{bmatrix} x^3+4x^2+3x+1 \\ 4x^2+2x+2 \end{bmatrix}\right)$	[0,0]	
$(v_3, u_3) = \left(\begin{bmatrix} 3x & x^2+x+1 \\ 2x^2+2x+1 & x^2+3x \end{bmatrix}, \begin{bmatrix} 4x^2+2x+4 \\ 2x^3+3x^2+4x+4 \end{bmatrix}\right)$	[1,1]	
$(v_4, u_4) = \left(\begin{bmatrix} x^2+2 & 2x+1 \\ 4x+2 & 2x^2+3x+2 \end{bmatrix}, \begin{bmatrix} x^3+4x+2 \\ 6x^2+6 \end{bmatrix}\right)$	[0,1]	
$(v_1, u_1) = \left(\begin{bmatrix} x^2+2x+3 & 2x+3 \\ x^2 & x \end{bmatrix}, \begin{bmatrix} x^3+2x^2+4x+5 \\ x^3+x+3 \end{bmatrix}\right)$	[0,1]	70
$(v_2, u_2) = \left(\begin{bmatrix} x^2+4x & 2x^2+3x+1 \\ x^2+2 & 2x+1 \end{bmatrix}, \begin{bmatrix} x^3+6x^2+5x+1 \\ x^3+4x+2 \end{bmatrix}\right)$	[0,0]	
$(v_3, u_3) = \left(\begin{bmatrix} x^2+x & x+1 \\ x^2+x+3 & 2x+2 \end{bmatrix}, \begin{bmatrix} x^3+x^2+x+2 \\ x^3+x^2+4x+6 \end{bmatrix}\right)$	[0,1]	
$(v_4, u_4) = \left(\begin{bmatrix} 2x+2 & x^2+2x+1 \\ x^2+x+2 & 2x+3 \end{bmatrix}, \begin{bmatrix} 3x^2+5x+6 \\ x^3+x^2+4x+3 \end{bmatrix}\right)$	[1,1]	
$(v_1, u_1) = \left(\begin{bmatrix} 3x+1 & x^2+x+1 \\ 4x & x^2+x+2 \end{bmatrix}, \begin{bmatrix} 4x^2+2x+1 \\ 5x^2+2x+6 \end{bmatrix}\right)$	[0,1]	67
$(v_2, u_2) = \left(\begin{bmatrix} x^2+2 & 2x+2 \\ 2x^2+2 & 3x+1 \end{bmatrix}, \begin{bmatrix} x^3+4x+2 \\ 2x^3+5x+3 \end{bmatrix}\right)$	[0,0]	
$(v_3, u_3) = \left(\begin{bmatrix} x^2+4x & 2x^2+3x \\ x+1 & 1 \end{bmatrix}, \begin{bmatrix} x^3+6x^2+5x \\ x^2+2 \end{bmatrix}\right)$	[0,0]	
$(v_4, u_4) = \left(\begin{bmatrix} 4x+2 & x^2+2x+3 \\ x^2+4x & 2x^2+3x+2 \end{bmatrix}, \begin{bmatrix} 5x^2+5x \\ x^3+6x^2+5x+4 \end{bmatrix}\right)$	[1,1]	
$(v_1, u_1) = \left(\begin{bmatrix} x^2+2x+3 & x^2+3x+1 \\ x^2+x & x+1 \end{bmatrix}, \begin{bmatrix} x^3+3x^2+6x+5 \\ x^3+x^2+x+5 \end{bmatrix}\right)$	[1,1]	63
$(v_2, u_2) = \left(\begin{bmatrix} x^2+x+2 & 2x+3 \\ x^2+x & x+1 \end{bmatrix}, \begin{bmatrix} x^3+x^2+4x+6 \\ x^3+x^2+x+5 \end{bmatrix}\right)$	[1,1]	
$(v_3, u_3) = \left(\begin{bmatrix} 2x^2+4 & 4x+2 \\ 2x^2+3 & 3x+1 \end{bmatrix}, \begin{bmatrix} 2x^3+x \\ 2x^3+5x+6 \end{bmatrix}\right)$	[1,1]	
$(v_1, u_1) = \left(\begin{bmatrix} x^2+2x+5 & 3x+4 \\ x^2+2x & x+2 \end{bmatrix}, \begin{bmatrix} x^3+2x^2+3 \\ x^3+2x^2+x+5 \end{bmatrix}\right)$	[1,1]	52
$(v_2, u_2) = \left(\begin{bmatrix} x^2+x & x+2 \\ x^2 & x \end{bmatrix}, \begin{bmatrix} x^3+x^2+x+2 \\ x^3+x+3 \end{bmatrix}\right)$	[0,1]	

Chipertext	Hasil	Data
$(v_3, u_3) = \left(\begin{bmatrix} 2x^2+2 & 3x+1 \\ x^2+2x+3 & 2x+3 \end{bmatrix}, \begin{bmatrix} 2x^3+5x+3 \\ x^3+2x^2+4x+4 \end{bmatrix}\right)$	[0,0]	
$(v_1, u_1) = \left(\begin{bmatrix} 2x^2+2x+1 & x^2+3x \\ x^2+2 & 2x+1 \end{bmatrix}, \begin{bmatrix} 2x^3+3x^2+4x+3 \\ x^3+4x+6 \end{bmatrix}\right)$	[1,1]	49
$(v_2, u_2) = \left(\begin{bmatrix} x^2 & x+1 \\ 2x^2 & 2x \end{bmatrix}, \begin{bmatrix} x^3+x+1 \\ 2x^3+2x \end{bmatrix}\right)$	[0,0]	
$(v_3, u_3) = \left(\begin{bmatrix} 2x^2+2x & x^2+3x \\ x^2+3 & 2x+1 \end{bmatrix}, \begin{bmatrix} 2x^3+3x^2+4x+1 \\ x^3+4x+5 \end{bmatrix}\right)$	[0,1]	
$(v_1, u_1) = \left(\begin{bmatrix} x^2+3x+5 & x^2+4x+3 \\ x^2+2 & 2x+1 \end{bmatrix}, \begin{bmatrix} x^3+4x^2+2x+1 \\ x^3+4x+3 \end{bmatrix}\right)$	[1,0]	44
$(v_2, u_2) = \left(\begin{bmatrix} x^2+4x & x^2+2x+3 \\ x^2+x+2 & 2x+2 \end{bmatrix}, \begin{bmatrix} x^3+5x^2+3x+5 \\ x^3+x^2+4x \end{bmatrix}\right)$	[1,1]	
$(v_3, u_3) = \left(\begin{bmatrix} x^2+2 & 2x+1 \\ x^2+2x+3 & x^2+3x+1 \end{bmatrix}, \begin{bmatrix} x^3+4x+2 \\ x^3+3x^2+6x+3 \end{bmatrix}\right)$	[0,0]	
$(v_1, u_1) = \left(\begin{bmatrix} 3x+1 & x^2+x+1 \\ 3x+2 & x^2+2x+2 \end{bmatrix}, \begin{bmatrix} 4x^2+2x+5 \\ 4x^2+5x+3 \end{bmatrix}\right)$	[1,0]	39
$(v_2, u_2) = \left(\begin{bmatrix} x^2+4x & 2x^2+3x+1 \\ x^2+2 & 2x+1 \end{bmatrix}, \begin{bmatrix} x^3+6x^2+5x \\ x^3+4x+6 \end{bmatrix}\right)$	[0,1]	
$(v_3, u_3) = \left(\begin{bmatrix} 2x^2+2 & 3x+1 \\ x^2+5 & 3x+2 \end{bmatrix}, \begin{bmatrix} 2x^3+5x+5 \\ x^3+1 \end{bmatrix}\right)$	[1,1]	
$(v_1, u_1) = \left(\begin{bmatrix} x^2+4x+1 & 2x^2+3x \\ 3x & x^2+x+1 \end{bmatrix}, \begin{bmatrix} x^3+6x^2+5x+4 \\ 4x^2+2x+1 \end{bmatrix}\right)$	[1,0]	34
$(v_2, u_2) = \left(\begin{bmatrix} x^2+4 & 3x+2 \\ x^2+x+5 & 3x+3 \end{bmatrix}, \begin{bmatrix} x^3+4 \\ x^3+x^2+6 \end{bmatrix}\right)$	[0,0]	
$(v_3, u_3) = \left(\begin{bmatrix} 2x^2+2x & x^2+3x \\ 4x+3 & x^2+2x+3 \end{bmatrix}, \begin{bmatrix} 2x^3+3x^2+4x+4 \\ 5x^2+5x+4 \end{bmatrix}\right)$	[1,0]	
$(v_1, u_1) = \left(\begin{bmatrix} x^2+5 & 3x+2 \\ 2x^2+4 & 4x+2 \end{bmatrix}, \begin{bmatrix} x^3+5 \\ 2x^3+x \end{bmatrix}\right)$	[0,1]	30
$(v_2, u_2) = \left(\begin{bmatrix} 2x & x^2+x+1 \\ 3x+4 & x^2+3x+3 \end{bmatrix}, \begin{bmatrix} 3x^2+2x+4 \\ 4x^2+x+1 \end{bmatrix}\right)$	[1,1]	
$(v_3, u_3) = \left(\begin{bmatrix} x^2+2x+2 & 2x+3 \\ 2x+3 & x+3 \end{bmatrix}, \begin{bmatrix} x^3+2x^2+4x \\ 2x^2+3x+5 \end{bmatrix}\right)$	[1,0]	
$(v_1, u_1) = \left(\begin{bmatrix} x^2+2x+5 & 3x+4 \\ 4x & x^2+x+2 \end{bmatrix}, \begin{bmatrix} x^3+2x^2+6 \\ 5x^2+2x+6 \end{bmatrix}\right)$	[0,1]	27
$(v_2, u_2) = \left(\begin{bmatrix} x^2+4 & 3x+3 \\ 2x & x^2+x \end{bmatrix}, \begin{bmatrix} x^3 \\ 3x^2+2x+1 \end{bmatrix}\right)$	[1,0]	
$(v_3, u_3) = \left(\begin{bmatrix} 4x & 2x^2+2x \\ 2x+5 & x^2+3x+2 \end{bmatrix}, \begin{bmatrix} 6x^2+4x+3 \\ 3x^2+x+1 \end{bmatrix}\right)$	[1,1]	

Chipertext	Hasil	Data
$(v_1, u_1) = \left(\begin{bmatrix} x^2+3 & 2x+1 \\ 2x^2+4 & 4x+2 \end{bmatrix}, \begin{bmatrix} x^3+4x+3 \\ 2x^3+x \end{bmatrix}\right)$	[0,1]	23
$(v_2, u_2) = \left(\begin{bmatrix} x^2+3x & x^2+2x+2 \\ x^2+2x+2 & 2x+3 \end{bmatrix}, \begin{bmatrix} x^3+4x^2+3x+2 \\ x^3+2x^2+4x \end{bmatrix}\right)$	[0,1]	
$(v_3, u_3) = \left(\begin{bmatrix} 3x & x^2+x+1 \\ 2x^2+2x+1 & x^2+3x \end{bmatrix}, \begin{bmatrix} 4x^2+2x+5 \\ 2x^3+3x^2+4x+3 \end{bmatrix}\right)$	[1,1]	
$(v_1, u_1) = \left(\begin{bmatrix} x^2+4x+1 & 2x^2+3x \\ x^2+4 & 3x+2 \end{bmatrix}, \begin{bmatrix} x^3+6x^2+5x \\ x^3+1 \end{bmatrix}\right)$	[0,1]	21
$(v_2, u_2) = \left(\begin{bmatrix} 3x & x^2+x+2 \\ 3x+4 & x^2+3x+3 \end{bmatrix}, \begin{bmatrix} 4x^2+2x+1 \\ 4x^2+x+2 \end{bmatrix}\right)$	[0,1]	
$(v_3, u_3) = \left(\begin{bmatrix} x^2+4x & 2x^2+3x \\ 4x+1 & 2x^2+2x \end{bmatrix}, \begin{bmatrix} x^3+6x^2+5x \\ 6x^2+4x+4 \end{bmatrix}\right)$	[0,1]	
$(v_1, u_1) = \left(\begin{bmatrix} x^2+4x+1 & 2x^2+3x \\ 3x+2 & x^2+2x+2 \end{bmatrix}, \begin{bmatrix} x^3+6x^2+5x+4 \\ 4x^2+5x+3 \end{bmatrix}\right)$	[1,0]	11
$(v_2, u_2) = \left(\begin{bmatrix} x^2+2x+2 & 2x+3 \\ x^2+4x+3 & x^2+3x+3 \end{bmatrix}, \begin{bmatrix} x^3+2x^2+4x+1 \\ x^3+5x^2+6x \end{bmatrix}\right)$	[1,1]	
$(v_1, u_1) = \left(\begin{bmatrix} x^2+4x+1 & x^2+2x+2 \\ 2x+4 & x^2+3x+2 \end{bmatrix}, \begin{bmatrix} x^3+5x^2+3x+2 \\ 3x^2+x+1 \end{bmatrix}\right)$	[0,1]	7
$(v_2, u_2) = \left(\begin{bmatrix} x^2+2x & x+2 \\ x^2+2x+5 & 3x+4 \end{bmatrix}, \begin{bmatrix} x^3+2x^2+x+5 \\ x^3+2x^2+3 \end{bmatrix}\right)$	[1,1]	
$(v_1, u_1) = \left(\begin{bmatrix} x^2+3x+5 & x^2+4x+3 \\ x^2+x+2 & 2x+2 \end{bmatrix}, \begin{bmatrix} x^3+4x^2+2x+2 \\ x^3+x^2+4x+3 \end{bmatrix}\right)$	[1,0]	2

Lampiran 3 *Script Code SageMath:* Proses Enkripsi

```
from random import randint, choice
import sqlite3
from sage.all import *

# === Parameter dan Ring ===
q = 277
R.<x> = PolynomialRing(ZZ)

# === Fungsi Polinomial dan Matriks Acak ===
def rand_poly():
    return randint(0, 20) * x + randint(0, 20)

def rand_matrix(rows, cols):
    return Matrix(R, rows, cols, [[rand_poly() for _ in
range(cols)] for _ in range(rows)])

def simple_noise_matrix(rows, cols):
    mat = Matrix(R, rows, cols, [[0 for _ in range(cols)]
for _ in range(rows)])
    i = randint(0, rows - 1)
    j = randint(0, cols - 1)
    mat[i, j] = choice([-1, 1])
    return mat

def rand_noise_matrix(rows, cols):
    return simple_noise_matrix(rows, cols)

# === Konversi Bilangan Bulat ke Matriks Pesan 2-bit ===
def int_to_message_blocks(n):
    binary = bin(n)[2:]
    if len(binary) % 2 != 0:
        binary = '0' + binary
    return [[[int(b1)], [int(b2)]] for b1, b2 in
zip(binary[::2], binary[1::2])]

# === Format Matriks Polinomial ke String Koefisien
Bersarang ===
def poly_matrix_to_formatted_string(mat):
    rows = []
    for row in mat:
        formatted_row = []
        for poly in row:
            deg = poly.degree()
            coeffs = [poly[i] for i in range(deg + 1)]
```

```
            coeff_str = '+'.join([str(c) if c >= 0 else f"-
{abs(c)}" for c in coeffs])
            formatted_row.append(coeff_str)
        rows.append(' '.join(formatted_row))
    return '[' + '],['.join(rows) + ']'

# === Inisialisasi Matriks A, s, e, b ===
while True:
    A = rand_matrix(2, 2)
    if A.det() != 0:
        break

s = rand_matrix(2, 1)
e = rand_noise_matrix(2, 1)
b = (A * s + e) % q

# === Enkripsi ===
def encrypt_messages(message_blocks):
    encrypted = []
    for idx, m in enumerate(message_blocks):
        r = rand_matrix(2, 2)
        e1 = rand_noise_matrix(2, 2)
        e2 = rand_noise_matrix(2, 1)
        m_mat = Matrix(R, m)
        m_prim = (q // 2) * m_mat
        v = (r * A + e1) % q
        u = (r * b + e2 + m_prim) % q

        print(f"\n--- Enkripsi blok ke-{idx+1} ---")
        print("Plaintext (bit):", m_mat)
        print("m' (scaled):\n", m_prim)
        print("v =\n", v)
        print("u =\n", u)

        encrypted.append((v, u))
    return encrypted

# === Simpan ke SQLite ===
def save_to_sqlite(cipher_list, s):
    conn = sqlite3.connect("enkripsifix.db")
    cursor = conn.cursor()

    cursor.execute("""
        CREATE TABLE IF NOT EXISTS ciphertexts (
            id INTEGER PRIMARY KEY AUTOINCREMENT,
            v TEXT,
            u TEXT
```

```
        )
    """)

    cursor.execute("""
        CREATE TABLE IF NOT EXISTS secret_key (
            id INTEGER PRIMARY KEY CHECK (id = 1),
            s TEXT
        )
    """)

    cursor.execute("DELETE FROM secret_key")
    s_str = poly_matrix_to_formatted_string(s)
    cursor.execute("INSERT INTO secret_key (id, s) VALUES
(1, ?)", (s_str,))

    for v, u in cipher_list:
        v_str = poly_matrix_to_formatted_string(v)
        u_str = poly_matrix_to_formatted_string(u)
        cursor.execute("INSERT INTO ciphertexts (v, u)
VALUES (?, ?)", (v_str, u_str))

    conn.commit()
    conn.close()
    print("✅ Ciphertext dan secret key berhasil disimpan ke
database (enkripsifix.db)")

# === Input dari Pengguna ===
print("Masukkan bilangan bulat (pisahkan dengan koma,
contoh: 504, 201, 90):")
raw_input = input(">> ")

try:
    int_list = [int(x.strip()) for x in raw_input.split(",")
if x.strip().isdigit()]
    if not int_list:
        raise ValueError("Tidak ada bilangan valid yang
dimasukkan.")

    all_blocks = []
    for number in int_list:
        blocks = int_to_message_blocks(number)
        all_blocks.extend(blocks)

    encrypted_list = encrypt_messages(all_blocks)

    print("\n===== PUBLIK KEY =====")
    print("A =\n", A)
```

```
    print("s =\n", s)
    print("b = A·s + e =\n", b)

    save_to_sqlite(encrypted_list, s)

except Exception as e:
    print("✗ Terjadi kesalahan:", e)
```

Lampiran 4 *Script Code SageMath:* Merubah Database ke Polinomial

```
import sqlite3
from sage.all import *

# Inisialisasi ring polinomial
R.<x> = PolynomialRing(ZZ)

# Fungsi ubah string koefisien jadi polinomial
def parse_coeff_string_to_poly(coeff_string):
    coeffs = list(map(int, coeff_string.split('+')))
    return sum([c * x^i for i, c in enumerate(coeffs)])

# Fungsi konversi string matriks ke Matrix polinomial
def parse_matrix_coeff_string(matrix_string):
    matrix_string = matrix_string.strip("[] ").replace("],",
"]@").split("@")
    result = []
    for row in matrix_string:
        row = row.strip("[] ")
        if not row:
            continue
        polys = row.split()
        row_data = [parse_coeff_string_to_poly(p) for p in
polys]
        result.append(row_data)

    # Ukuran matriks
    rows = len(result)
    cols = len(result[0]) if rows > 0 else 0
    return Matrix(R, rows, cols, result)

# Fungsi baca dari file database dan tampilkan sebagai
polinomial
def read_and_convert_from_db(db_path="enkripsifix.db"):
    conn = sqlite3.connect(db_path)
    cursor = conn.cursor()

    # Ambil semua ciphertexts
    cursor.execute("SELECT v, u FROM ciphertexts")
    data = cursor.fetchall()

    # Ambil secret key
    cursor.execute("SELECT s FROM secret_key WHERE id = 1")
    s_data = cursor.fetchone()

    conn.close()
```

```
    print("✅ Membaca data dari database...\n")

    for idx, (v_str, u_str) in enumerate(data):
        print(f"\n🔐 Ciphertext blok ke-{idx+1}")
        v = parse_matrix_coeff_string(v_str)
        u = parse_matrix_coeff_string(u_str)
        print("v =\n", v)
        print("u =\n", u)

    if s_data:
        s = parse_matrix_coeff_string(s_data[0])
        print("\n🔑 Secret key (s) =\n", s)
    else:
        print("\n⚠️ Tidak ditemukan secret key.")

# === MAIN ===
read_and_convert_from_db("enkripsifix.db")  # Ganti nama
file kalau perlu
```

Lampiran 5 *Script Code SageMath:* Proses Dekripsi

```
import sqlite3
from sage.all import *

# === Parameter ===
q = 277
R.<x> = PolynomialRing(ZZ)

# === Konversi String Koefisien ke Polinomial ===
def parse_coeff_string_to_poly(coeff_string):
    coeffs = list(map(int, coeff_string.split('+')))
    return sum([c * x^i for i, c in enumerate(coeffs)])

def parse_matrix_coeff_string(matrix_string):
    matrix_string = matrix_string.strip("[] ").replace("],",
"]@").split("@")
    result = []
    for row in matrix_string:
        row = row.strip("[] ")
        if not row:
            continue
        polys = row.split()
        row_data = [parse_coeff_string_to_poly(p) for p in
polys]
        result.append(row_data)

    rows = len(result)
    cols = len(result[0]) if rows > 0 else 0
    return Matrix(R, rows, cols, result)

# === Fungsi Dekripsi dan Simpan Hasil ===
def decrypt_and_save_to_db(db_path="enkripsifix.db"):
    conn = sqlite3.connect(db_path)
    cursor = conn.cursor()

    # Ambil data ciphertext
    cursor.execute("SELECT v, u FROM ciphertexts")
    data = cursor.fetchall()

    # Ambil secret key
    cursor.execute("SELECT s FROM secret_key WHERE id = 1")
    s_data = cursor.fetchone()

    if not s_data:
        print("❌ Secret key tidak ditemukan.")
        conn.close()
```

```
        return

    s = parse_matrix_coeff_string(s_data[0])

    # Buat ulang tabel hasil dekripsi
    cursor.execute("DROP TABLE IF EXISTS decrypted_bits")
    cursor.execute("""
        CREATE TABLE decrypted_bits (
            id INTEGER PRIMARY KEY AUTOINCREMENT,
            bit1 INTEGER,
            bit2 INTEGER
        )
    """)

    print("🔑 Secret Key s =\n", s)
    print("\n=== PROSES DEKRIPSI ===")

    for idx, (v_str, u_str) in enumerate(data):
        v = parse_matrix_coeff_string(v_str)
        u = parse_matrix_coeff_string(u_str)

        m_prim = (u - v * s) % q
        m_scaled = m_prim.apply_map(lambda poly:
poly.coefficients(sparse=False)[0])
        m_bit = m_scaled.apply_map(lambda val: int(round(val
/ (q // 2))) % 2)

        # Ambil dua bit dari hasil 2x1
        bit1 = int(m_bit[0][0])
        bit2 = int(m_bit[1][0])

        cursor.execute("INSERT INTO decrypted_bits (bit1,
bit2) VALUES (?, ?)", (bit1, bit2))

        print(f"\n💠 Ciphertext ke-{idx+1}")
        print("m' =\n", m_prim)
        print("Bit =\n", m_bit)

    conn.commit()
    conn.close()
    print("\n✅ Semua hasil dekripsi telah disimpan ke tabel
'decrypted_bits' di database.")

# === MAIN ===
decrypt_and_save_to_db("enkripsifix.db")
```

Lampiran 6 *Script Code Phyton:* Merubah Biner ke Bilangan Bulat

```
def biner_ke_integer(biner_str):
    try:
        # Mengubah string biner ke bilangan bulat
        angka = int(biner_str, 2)
        return angka
    except ValueError:
        print("Input bukan biner yang valid (hanya boleh 0
dan 1).")
        return None

# Contoh penggunaan
biner = input("Masukkan bilangan biner: ")
hasil = biner_ke_integer(biner)

if hasil is not None:
    print(f"Bilangan bulatnya: {hasil}")
```

RIWAYAT HIDUP

Riza Ivania Indah Ravelina, lahir di Kabupaten Pasuruan pada tanggal 01 Mei 2003. Biasa dipanggil Riza. Bertempat tinggal di Dusun Nampes, Desa Nogosari, Kecamatan Pandaan, Kabupaten Pasuruan, Gg.01, No. 16F Rt.03 RW.02 Provinsi Jawa Timur. Merupakan putri ketiga dari Bapak Muhammad Jainul dan Ibu Ruli Erni Astuti serta mempunyai dua kakak perempuan bernama Erlian Desi Ririanti dan Andriani Virga Kusumawardani.

Jenjang pendidikannya dimulai sejak bersekolah di TK Aisyiyah Bustanul Athfal Pandaan di Jl. Sultan Agung No.557, Desa Pesantren, Kecamatan Pandaan yang lulus pada tahun 2009. Setelah itu melanjutkan di SDN Pandaan II dan lulus tahun 2015. Pendidikan selanjutnya ditempuh di SMPN 1 Pandaan dan lulus tahun 2018. Kemudian melanjutkan pendidikan di SMAN 1 Purwosari dan lulus tahun 2021. Pada jenjang perguruan tinggi, ia melanjutkan pendidikannya dengan berkuliah di Universitas Islam Negeri Maulana Malik Ibrahim Malang dengan menekuni bidang Matematika murni di Fakultas Sains dan Teknologi.

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

BUKTI KONSULTASI SKRIPSI

Nama : Riza Ivania Indah Ravelina
NIM : 210601110073
Fakultas / Jurusan : Sains dan Teknologi / Matematika
Judul Skripsi :Implementasi *Module Learning with Errors* pada Pengamanan Data Transaksi PT. Indonesia Comnet Plus Surabaya
Pembimbing I : Muhammad Khudzaifah, M.Si.
Pembimbing II : Abdul Aziz, M.Si.

No	Tanggal	Hal	Tanda Tangan
1.	7 Agustus 2024	Konsultasi Topik dan Data	1.
2.	7 Oktober 2024	Konsultasi Bab I, II, dan III	2.
3.	29 Oktober 2024	Konsultasi Bab I, II, dan III	3.
4.	25 November 2024	Konsultasi Bab I, II, dan III	4.
5.	16 Desember 2024	Konsultasi Bab I, II, dan III	5.
6.	17 Desember 2024	Konsultasi Kajian Agama Bab I dan II	6.
7.	9 Januari 2025	ACC Bab I, II, dan III	7.
8.	9 Januari 2025	ACC Kajian Agama Bab I dan II	8.
9.	20 Januari 2025	ACC Seminar Proposal	9.
10.	26 Maret 2025	Konsultasi Revisi Seminar Proposal	10.
11.	13 April 2025	Konsultasi Bab IV dan V	11.
12.	22 April 2025	Konsultasi Bab IV dan V	12.
13.	25 April 2025	ACC Bab IV dan V	13.
14.	29 April 2025	ACC Seminar Hasil	14.

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

15.	6 Mei 2025	Konsultasi Kajian Agama Bab IV	15.
16.	14 Mei 2025	ACC Kajian Agama Bab IV	16.
17.	2 Juni 2025	ACC Sidang Skripsi	17.
18.	2 Juni 2025	ACC Keseluruhan Kajian Agama	18.
19.	10 Juni 2025	ACC Keseluruhan	19.

Malang, 10 Juni 2025
Mengetahui,
Ketua Program Studi Matematika

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