SKRIPSI

SISTEM KRIPTOGRAFI KUNCI PUBLIK *RING LEARNING WITH ERRORS* (RLWE) ATAS RING POLINOMIAL

RIRIN RIA ARYANI

22106010024

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2026

SISTEM KRIPTOGRAFI KUNCI PUBLIK *RING LEARNING WITH ERRORS* (RLWE) ATAS RING POLINOMIAL

Skripsi

Untuk memenuhi sebagian persyaratan

mencapai derajat Sarjana S-1

Program Studi Matematika

diajukan oleh

RIRIN RIA ARYANI

22106010024

Kepada

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2026

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi / Tugas Akhir
Lamp : 1 Bendel Skripsi

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : Ririn Ria Aryani
NIM : 22106010024
Judul Skripsi : Sistem Kriptografi *Ring Learning With Errors* (RLWE) atas Ring Polinomial.

sudah dapat diajukan kembali kepada Program Studi Matematika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Program Studi Matematika.

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqasyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 18 Mei 2026
Pembimbing,

M. Zaki Riyanto, S.Si., M.Sc.
NIP. 19840113 201503 1 001

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-1201/Un.02/DST/PP.00.9/06/2026

Tugas Akhir dengan judul : Sistem Kriptografi Kunci Publik Ring Learning With Errors (RLWE) atas Ring Polinomial

yang dipersiapkan dan disusun oleh:

Nama : RIRIN RIA ARYANI
Nomor Induk Mahasiswa : 22106010024
Telah diujikan pada : Rabu, 03 Juni 2026
Nilai ujian Tugas Akhir : A

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Muhamad Zaki Riyanto, S.Si., M.Sc.
SIGNED

Valid ID: 6a22392f39f62

Penguji I

Arif Munandar, M.Sc.
SIGNED

Valid ID: 6a22430f33a68

Penguji II

Pipit Pratiwi Rahayu, S.Si., M.Sc.
SIGNED

Valid ID: 6a20e79df1a4d

Yogyakarta, 03 Juni 2026
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

Prof. Dr. Dra. Hj. Khurul Wardati, M.Si.
SIGNED

Valid ID: 6a224d5698b78

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini:

Nama	: Ririn Ria Aryani
NIM	: 22106010024
Program Studi	: Matematika
Fakultas	: Sains dan Teknologi

Dengan ini, saya menyatakan bahwa dalam skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu Perguruan Tinggi dan sesungguhnya skripsi ini merupakan hasil pekerjaan penulis sendiri sepanjang pengetahuan penulis, bukan duplikasi atau saduran dari karya orang lain kecuali bagian tertentu yang penulis ambil sebagai bahan acuan. Apabila terbukti pernyataan ini tidak benar, sepenuhnya menjadi tanggung jawab penulis.

Yogyakarta, 25 Mei 2026

Ririn Ria Aryani

22106010024

HALAMAN PERSEMBAHAN

Dipersembahkan:

bagi kedua orang tua dan UIN Sunan Kalijaga

Yogyakarta, sebagai bentuk bakti kecil penulis.

HALAMAN MOTTO

”Remember your points. Take the rules and note the pat(h)tern.

Find the pieces, then complete your puzzle.”

”Kenali mengapa-mu, api luar hanya sia-sia tanpa pemantik anala dari dalam.”

”Ka luhur tong sieun ku gugur, ka handap tong sieun ku cacing.

Suntukkeun asma Pangeran dina saban léngkah-laku salira.”

(”Ke langit tak perlu gentar oleh guntur, ke tanah tak usah gelisah oleh cacing.

Hadirkan Tuhan dalam setiap langkah-lakumu.”)

-R

PRAKATA

Alhamdulillaahirabbil'aalamiin, puji syukur ke hadirat Allah SWT. yang telah memberikan rahmat, nikmat, serta hidayah-Nya kepada penulis, sehingga penulis dapat menyelesaikan skripsi dengan judul "Sistem Kriptografi Kunci Publik *Ring Learning with Errors* (RLWE) atas Ring Polinomial" sebagai salah satu tugas akhir dan prasyarat mencapai gelar Sarjana Matematika.

Penulis menyadari bahwa penulisan skripsi ini terdapat banyak hambatan dan halangan. Namun berkat adanya motivasi, bantuan, bimbingan, dan dorongan dari berbagai pihak, *alhamdulillah* skripsi ini dapat terselesaikan. Oleh karena itu, dengan kerendahan hati penulis menyampaikan terima kasih kepada:

1. Bapak Prof. Noorhaidi, S.Ag., M.A., M.Phil., Ph.D., selaku pimpinan dan Rektor Universitas Islam Negeri Sunan Kalijaga Yogyakarta.

2. Ibu Prof. Dr. Dra. Hj. Khurul Wardati, M.Si., Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga, serta selaku dosen pembimbing akademik, atas arahannya selama penulis menempuh pendidikan.

3. Ibu Dr. Epha Diana Supandi, S.Si., M.Sc., Ketua Program Studi Matematika Universitas Islam Negeri Sunan Kalijaga.

4. Bapak M. Zaki Riyanto, S.Si., M.Sc., selaku dosen pembimbing skripsi yang telah menyediakan waktu, tenaga, dan pikiran untuk membimbing penulis dalam penyusunan skripsi ini.

5. Bapak Arif Munandar M.Sc. & Ibu Pipit Pratiwi Rahayu, S.Si., M.Sc., selaku

dosen penguji yang telah memberikan masukan dan saran untuk perbaikan tugas akhir ini.

6. Seluruh dosen dan staf Fakultas Sains dan Teknologi yang telah memberikan ilmu bermanfaat dan memberikan pelayanan administrasi akademik.
7. Kedua orang tua, para adik, dan segenap keluarga atas segala doa, dukungan, dan nasihat yang senantiasa mengiringi.
8. Rekan-rekan organisasi, khususnya bagi Himpunan Program Studi (HMPS) Matematika, serta Forum Kajian Islam dan Sains Teknologi (FKIST) sebagai salah dua wadah berproses dan berkembang penulis.
9. Seluruh rekan Program Studi Matematika 2022, rekan KKN-200 Angk.117 UIN Sunan Kalijaga, serta rekan-rekan terdekat yang senantiasa dapat di-andalkan dan berperan dalam berbagai hal.
10. Seluruh pihak yang tidak dapat penulis sebutkan secara langsung maupun tidak langsung dalam proses penyelesaian tugas akhir ini.

Tugas akhir ini sejatinya tidaklah sempurna, sehingga segala masukan untuk pengembangan kajian di masa mendatang sangatlah diharapkan. Penulis berharap pula semoga skripsi ini dapat memberikan manfaat bagi seluruh pihak, terlebih bagi para pembaca. Terima kasih.

Yogyakarta, 03 Juni 2026

Ririn Ria Aryani

NIM. 22106010024

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMBANG

$x \in A$	:	x anggota A
$A \subseteq X$	:	A himpunan bagian (*subset*) atau sama dengan X
$\mathbb{N}$	:	himpunan semua asli
$\mathbb{Z}$	:	himpunan semua bilangan bulat
$\mathbb{Z}^{>0}$	:	himpunan semua bilangan bulat positif
$\mathbb{Z}_q$	:	himpunan bilangan bulat modulo q
$\mathbb{R}$	:	himpunan semua bilangan real
$\blacksquare$	:	akhir suatu bukti
$\sum_{i=1}^{n} a_i$	:	penjumlahan $a_1 + a_2 + \cdots + a_n$
$\prod_{i=1}^{n} a_i$	:	perkalian $a_1 \cdot a_2 \cdot \cdots \cdot a_n$
$a \mid b$	:	a membagi habis b
$a \nmid b$	:	a tidak membagi habis b
$e_k : \mathcal{P} \to \mathcal{C}$	:	Fungsi enkripsi yang memetakan *plaintext* ke *ciphertext*.
$d_k : \mathcal{C} \to \mathcal{P}$	:	Fungsi dekripsi yang memetakan *ciphertext* kembali ke *plaintext*.

INTISARI

SISTEM KRIPTOGRAFI KUNCI PUBLIK

RING LEARNING WITH ERRORS (RLWE)

ATAS RING POLINOMIAL

Oleh

Ririn Ria Aryani

22106010024

Ring Learning with Errors (RLWE) diperkenalkan oleh Lyubashevsky, Peikert, dan Regev pada 2010 lalu. Dalam perkembangannya, RLWE jadi salah satu kandidat kuat standardisasi kriptografi pasca-kuantum berbasis latis atau kisi (*lattice-based*). Hadirnya RLWE didasari oleh kemunculan komputasi kuantum, seperti algoritma Shor yang mampu memfaktorkan bilangan besar secara cepat, sehingga keamanan pada sistem kriptografi kunci publik klasik seperti RSA dan ECC juga mulai terancam. Penelitian ini difokuskan pada mekanisme kerja sistem kriptografi kunci publik RLWE dalam ring $R_q = Z_q[x]/\langle x^n + 1\rangle$, dengan q berupa modulus bilangan prima dan $n = 2^k$, dengan $k \in \mathbb{Z}$. Mekanisme ini meliputi proses pembangkitan kunci, enkripsi, dan dekripsi pesan. Selain dikaji secara manual, pada implementasi skema tersebut pula dikaji secara komputasi menggunakan perangkat lunak SageMath.

Kata kunci: Kriptografi Berbasis Latis, Kriptografi Kunci Publik, RLWE (*Ring Learning with Errors*), Ring Polinomial, SageMath.

ABSTRACT

PUBLIC KEY CRYPTOGRAPHY SYSTEM

RING LEARNING WITH ERRORS (RLWE) OVER POLYNOMIAL RINGS

By

Ririn Ria Aryani

22106010024

Ring Learning with Errors (RLWE) was introduced by Lyubashevsky, Peikert, and Regev in 2010. In its development, RLWE has become a strong candidate for post-quantum cryptographic standardisation based on lattices. The emergence of RLWE is driven by the advent of quantum computing, such as Shor's algorithm, which is capable of factoring large numbers rapidly, thereby threatening the security of classical public-key cryptographic systems such as RSA and ECC. This research focuses on the working mechanism of the RLWE public-key cryptographic system in the ring $R_q = Z_q[x]/\langle x^n + 1\rangle$, where q is a prime modulus and $n = 2^k$, with $k \in \mathbb{Z}$. This mechanism encompasses the processes of key generation, encryption, and message decryption. In addition to being examined manually, the implementation of this scheme was also analysed computationally using the SageMath as software.

Keywords: Lattice-based Cryptography, Public-Key Cryptography, RLWE (Ring Learning with Errors), Ring Polynomials, SageMath.

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Dalam era digital seperti saat ini, ancaman kebocoran data, penipuan siber, hingga spionase digital menjadi tantangan yang selalu ada. Seluruh data mulai dari data di media sosial hingga perbankan *online* dan keamanan nasional tiada hentinya dikirimkan melalui jaringan global. Menurut laporan IBM tahun 2023, biaya rata-rata kebocoran data di tahun tersebut mencapai nominal $4.45 juta, hal tersebut menunjukkan bahwa mekanisme kekuatan dalam perlindungan data masih sangat diperlukan (Mohan et al., 2025).

Lebih lanjut, prediksi IBM untuk 2025 menekankan bahwa adanya ancaman baru saat ini seperti pemanfaatan *generatif Artificial Intelligence* (AI), komputasi kuantum terhadap sistem enkripsi kunci publik modern pun semakin meningkatkan urgensi transisi menuju sistem kriptografi *quantum-safe* (International Business Machines Corporation (IBM), 2024). Tren ini berlanjut pada prediksi IBM 2026 yang menyoroti semakin kompleksnya penggunaan AI dalam serangan siber, dan pentingnya identitas digital, serta kebutuhan *crypto agility* untuk mempercepat modernisasi manajemen kriptografi (International Business Machines Corporation (IBM), 2025). Untuk memahami hal tersebut, perlu ditinjau kembali perkembangan kriptografi sebagai salah satu solusi utama yang digunakan dalam persoalan ini.

Seiring berkembangnya teknologi sebagaimana dipaparkan di atas, masa ini penggunaan kriptografi modern awal seperti DES atau *Data Encryption Standard*

secara bertahap ditinggalkan karena dianggap sudah tidak lagi lebih aman. Sebagai alternatif, algoritma kriptografi yang lebih modern kemudian dikembangkan dengan tingkat keamanan dan efisiensi yang lebih tinggi, sehingga kecil kemungkinan diselesaikan oleh komputer klasik.

Secara umum, kriptografi modern diklasifikasikan ke dalam dua kategori utama, yakni kriptografi simetris dan asimetris (Cynthia et al., 2026). Pertama, pada kriptografi simetris digunakan kunci yang sama untuk mengenkripsi ataupun mendekripsi pesan. Pada sistem ini, AES (*Advanced Encryption Standard*) menjadi salah satu algoritma yang banyak digunakan dan dianggap aman dengan kecepatan komputasi yang tinggi dalam pengoperasiannya (Baso & Anriani, 2024). Namun karena hanya digunakan satu kunci yang sama, kriptografi simetris memiliki risiko tinggi dalam pendistribusian kuncinya. Setiap kali kunci dibagikan, akan selalu ada risiko penyadapan oleh pihak ketiga yang tidak diinginkan.

Untuk mengatasi masalah tersebut, dikembangkan kriptografi asimetris yang menggunakan sepasang kunci, yaitu kunci publik untuk enkripsi dan kunci rahasia untuk skema dekripsi, sehingga keamanan data dapat tetap terjaga walaupun apabila kunci publik telah diketahui umum (Douglas & Paterson, 2019). Pada kriptografi asimetris, algoritma yang paling umum dan populer digunakan saat ini yaitu RSA (Rivest-Shamir-Adleman) dengan penggunaan metode yang lebih aman. Sistem keamanannya didasarkan pada sulitnya pemfaktoran bilangan-bilangan yang besar jadi faktor-faktor prima. Hal tersebut dianggap mustahil diselesaikan dalam waktu yang singkat (Chandra, 2016).

Selain itu, adapun ECC (*Elliptic Curve Cryptography*) yang mengandalkan logaritma diskret sebagai dasar keamanannya. Algoritma ini dianggap memiliki keamanan lebih tinggi daripada jenis algoritma lain dan menawarkan penggunaan

ukuran kunci yang jauh lebih kecil (Wohlwend, 2016).

Pada dasarnya, kriptografi simetris dan asimetris dirancang sehingga dapat menghadapi ancaman serangan komputasional seperti *Brute force,* yaitu metode yang dilakukan dengan melakukan percobaan terhadap seluruh kemungkinan kunci hingga ditemukan solusi yang benar. Ketahanan suatu algoritma terhadap serangan tersebut bergantung pada ukuran kunci dan kemampuan komputasi yang diperlukan untuk menghasilkan dan menguji seluruh kemungkinan. Dalam hal ini, peningkatan panjang kunci dapat menjadi strategi utama dalam memperkuat sistem terhadap serangan komputer klasik (Kumar, 2022).

Akan tetapi, kemunculan komputasi kuantum mulai mengancam keamanan protokol-protokol kriptografi tersebut. Algoritma kuantum seperti algoritma Shor terbukti mampu memanfaatkan kekuatan *quantum bit* (*qubit*) untuk menyelesaikan suatu masalah matematis yang menjadi dasar keamanan saat ini secara efisien. Hal ini mencakup pemfaktoran bilangan besar pada RSA dan masalah logaritma diskret pada ECC yang banyak digunakan di perangkat seluler dan sistem *blockchain*. Ketidakmampuan sistem tersebut dalam menghadapi algoritma Shor sehingga mengakibatkan keamanan sistem kriptografi tersebut menjadi lebih rentan dan kurang memadai (Shor, 1994); (Nwaga & Nwagwughiagwu, 2024).

Ancaman ini bukan lagi sekadar spekulasi semenjak Google mengumumkan pencapaian *Quantum Supremacy* pada 2019 melalui prosesor kuantum Sycamore. Google mendemonstrasikan bahwa prosesor tersebut mampu menyelesaikan tugas tertentu dalam 200 detik. Sebagai perbandingan, diperlukan waktu hingga 10.000 tahun untuk tugas yang sama jika diselesaikan oleh komputer tercepat pada saat itu sekalipun (Arute et al., 2019). Karena risiko tersebut, pedoman keamanan digital menyarankan untuk beralih dari RSA dan ECC mulai tahun 2025, terutama untuk

data-data sensitif. Dalam hal ini, penggunaan *post-quantum cryptography* sangat direkomendasikan untuk digunakan lebih lanjut sebelum tahun 2030 sebagai solusi untuk menjamin keamanan data jangka panjang (Scrivano, 2025).

Menanggapi hal tersebut, *National Institute of Standards and Technology* (NIST) telah memulai proses standardisasi algoritma *Post-Quantum Cryptography* (PQC) dengan teliti. Di antara kandidat yang ada, kriptografi berbasis latis (*lattice-based cryptography*) hadir sebagai pendekatan paling menjanjikan. Hal ini tampak dari jumlah algoritma terbanyak yang diumumkan oleh NIST putaran ketiga yang termasuk kelompok algoritma kriptografi berbasis latis. Keamanan sistem berbasis latis tersebut didasarkan pada suatu permasalahan matematis dalam kisi $n-$dimensi, seperti *Shortest Vector Problem* (SVP) yang diyakini sulit dipecahkan, baik oleh komputer klasik maupun komputer kuantum ((Kumar, 2022); (Opiłka, Filip et al., 2024)).

Salah satu skema yang paling efisien dalam kategori ini ialah *Learning with Errors* (LWE) yang diperkenalkan oleh Oded Regev pada tahun 2005 sebagai permasalahan komputasi yang terbukti sulit dan memiliki reduksi keamanan terhadap *worst-case hardness* pada latis seperti *Shortest Vector Problem* (SVP) dan *Shortest Independent Vectors Problem* (SIVP) (Regev, 2010). Secara umum, LWE berada pada ruang vektor $\mathbb{Z}_q^n$ dengan menambahkan *noise* pada hasil perkalian linearnya, sehingga dapat dibentuk *search-problem* yang sulit diselesaikan tanpa mengetahui kunci rahasia (Peikert, 2016).

Namun meskipun demikian, menurut (Lindner & Peikert (2011)), skema LWE memiliki kelemahan pada ukuran kunci yang sangat besar, sehingga sulit diimplementasikan pada sistem dengan memori terbatas. Untuk mengatasi kendala tersebut, kemudian dikembangkan varian *Ring Learning with Errors* (RLWE) atas

ring polinomial oleh Lyubashevsky et al. (2010) yang mentransformasikan suatu permasalahan LWE dari struktur ruang vektor menjadi struktur ring polinomial. Secara umum, ring tersebut berbentuk $R_q = \mathbb{Z}_q[x]/\langle f(x)\rangle$, dengan $f(x) = x^n + 1$ untuk suatu n pangkat dari dua. Dengan memanfaatkan ring polinomial tersebut, RLWE mampu menawarkan ukuran kunci yang jauh lebih ringkas dan kecepatan operasi yang lebih tinggi tanpa mengurangi tingkat keamanannya.

1.2. Rumusan Masalah

Berdasarkan latar belakang di atas, persoalan-persoalan penelitian ini dapat dirumuskan sebagai berikut.

1. Bagaimana konsep-konsep dasar aljabar terkait yang melandasi ring RLWE $R_q = \mathbb{Z}_q/\langle x^n + 1\rangle$?
2. Bagaimana mekanisme sistem kriptografi kunci publik pada *Ring Learning with Errors*(RLWE), yakni meliputi proses pembangkitan kunci, enkripsi, dan dekripsi?
3. Bagaimana implementasi sederhana sistem kriptografi RLWE menggunakan SageMath?

1.3. Batasan Masalah

Agar pembahasan dalam penelitian ini tidak meluas, maka ditetapkan ruang lingkup atau batasan masalah sebagai berikut.

1. Penelitian ini berfokus pada konsep dasar ring, khususnya pada ring faktor $R_q = \mathbb{Z}_q[x]/\langle x^n + 1\rangle$ dengan q bilangan prima dan n merupakan pangkat dari dua.

2. Penelitian ini dibatasi pada sistem kriptografi kunci publik *Ring Learning with Errors* (RLWE), meliputi pembangkitan kunci, enkripsi, dan dekripsi, serta contoh sederhana dengan bantuan perangkat lunak SageMath.

1.4. Tujuan Penelitian

Pada penelitian ini, terdapat beberapa tujuan penelitian sebagai berikut.

1. Untuk mengkaji konsep-konsep aljabar dasar yang melandasi ring pada RLWE, yakni $R_q = \mathbb{Z}_q[x]/\langle x^n + 1\rangle$.
2. Untuk mengkaji mekanisme pada sistem kriptografi kunci publik RLWE.
3. Untuk memberikan contoh implementasi sederhana dari sistem kriptografi RLWE menggunakan perangkat lunak SageMath.

1.5. Manfaat Penelitian

Adapun manfaat dari penelitian ini yakni sebagai berikut.

1. Manfaat Teoretis

   Hasil pengkajian ini diharapkan dapat digunakan sebagai salah satu literatur ataupun referensi bagi pengembangan penelitian serupa.

2. Manfaat Praktis

   a. Memberikan pemahaman mengenai struktur aljabar yang terlibat pada sistem kriptografi RLWE.

   b. Memberikan pemahaman mengenai mekanisme sistem kriptografi RLWE dalam proses pembentukan kunci, enkripsi, dan dekripsi.

1.6. Tinjauan Pustaka

Ring Learning with Errors (RLWE) merupakan suatu perluasan dari LWE (*Learning with Errors*), suatu konsep yang diperkenalkan oleh Oded Regev pada 2005. Masalah RLWE dijanjikan dapat berpotensi besar untuk membuat kriptografi berbasis latis menjadi lebih praktis. Sistem RLWE dikonstruksi dengan konsep ring faktor atas ideal yang dibangun pada ring polinomial $\mathbb{Z}_q[x]$ dengan q bilangan prima dan ring $I = \langle f(x) \rangle = x^n + 1$ dengan $x^n \equiv -1 \pmod{q}$.

Misalkan terdapat dua pihak yang disebut sebagai Alice dan Bob. Dalam hal ini, Bob bertugas dalam pembangkitan kunci, yaitu membuat kunci publik a dan menghitung kunci publik $b = a \cdot s + e$ setelah sebelumnya ditentukan pula kunci rahasia $s \in R_q$ dan nilai *error* $e \in R_q$. Kemudian, dengan menggunakan kunci publik yang dibuat Bob, Alice dapat mengirim pesan terenkripsi c_k. Untuk mengetahui pesan yang dikirim Alice, Bob dapat melakukan proses dekripsi atau mengembalikan pesan asli d_k.

RLWE semakin terkenal melalui publikasi artikel Lyubashevsky et al. (2010) berjudul *"On Ideal Lattices and Learning with Errors over Rings*" oleh suatu tim peneliti yang beranggotakan Lyubashevski, Peikert, dan Regev pada 2010 silam. Dalam artikel tersebut, diperkenalkan algoritma pertukaran kunci pada RLWE yang kemudian dioptimalkan implementasinya oleh Erdem Alkim, Léo Ducas, Thomas Pöppelmann, dan Peter Schwabe pada Alkim et al. (2015). Adapun Ivan Blanco-Chacon pada Chacón (2020), dibahas kaitan antara RLWE sebagai kriptografi pasca-kuantum dengan *machine learning* serta teori bilangan. Pada artikel ini, dipaparkan mengenai beberapa implementasi, misalnya pengujian RLWE oleh Google yang dikembangkan lebih lanjut oleh Intel Labs dan MIRACLE Labs. Dari penelitian ini, terdapat *open problems* yang dapat dikaji lebih jauh, terutama dalam hal pemilihan

parameter keamanan dan hubungan yang lebih dalam dengan teori bilangan.

Sementara itu, sistem kriptografi terkait enkripsi dan dekripsi suatu pesan telah dibahas pada artikel yang disusun oleh Sitohang et al. (2024). Berdasarkan artikel tersebut, dikatakan bahwa algoritma RLWE menawarkan tingkat keamanan tinggi untuk skema kriptografi tersebut, terutama dalam menghadapi ancaman dari komputer kuantum. Pada hal ini, digunakan ring polinomial untuk pembangkitan kunci, dengan kunci pribadi dipilih secara acak dan pasangan kunci publik yang dihitung menggunakan kombinasi polinomial acak dan *noise*.

Adanya *noise* tersebut dapat membuat pemecahan kunci pribadi jadi lebih sulit, sehingga ketahanan terhadap serangan pun meningkat. Untuk dapat lebih dipahami, dalam artikel tersebut pula dibuat contoh implementasi sederhana dengan menggunakan $q = 17$, polinomial modulus $f(x) = x^2 + 1$, serta kunci pribadi dan polinomial acak yang telah ditentukan. Hasil percobaan menunjukkan bahwa pesan dapat didekripsi dengan akurat menggunakan kunci pribadi, sehingga hal ini dapat membuktikan keberhasilan algoritma RLWE terhadap keamanan data.

Terdapat pula beberapa penelitian terbaru mengenai topik terkait, seperti yang dilakukan oleh Koen de Boer dan Wessel van Woerden yang melakukan survei keamanan terhadap beberapa finalis NIST berbasis latis, salah satunya RLWE. Pada survei tersebut, dijumpai bahwa kompleksitas waktu yang digunakan pada RLWE lebih efisien daripada LWE biasa. Selain itu, ditemukan bahwa dari segi struktur di antara tiga varian LWE yang dibahas pada survei tersebut, RLWE merupakan varian paling terstruktur, LWE standar sebagai varian paling tidak terstruktur, sementara Module-LWE berada di antara keduanya (de Boer & van Woerden (2025)).

Kemudian pada seleksi NIST putaran ke-3, dari finalis alternatif algoritma KEM (keamanan kunci enkripsi), ukuran kunci publik berbasis latis tak terstruktur seperti LWE hampir sepuluh kali lebih besar daripada algoritma yang berbasis latis

terstruktur seperti RLWE dan MLWE. Sementara itu, LWE dan RLWE memiliki ruang kunci yang setara dengan total sejumlah q^n kemungkinan kunci rahasia yang berbeda (Regev, 2010); (Lyubashevsky et al., 2010).

1.7. Metode Penelitian

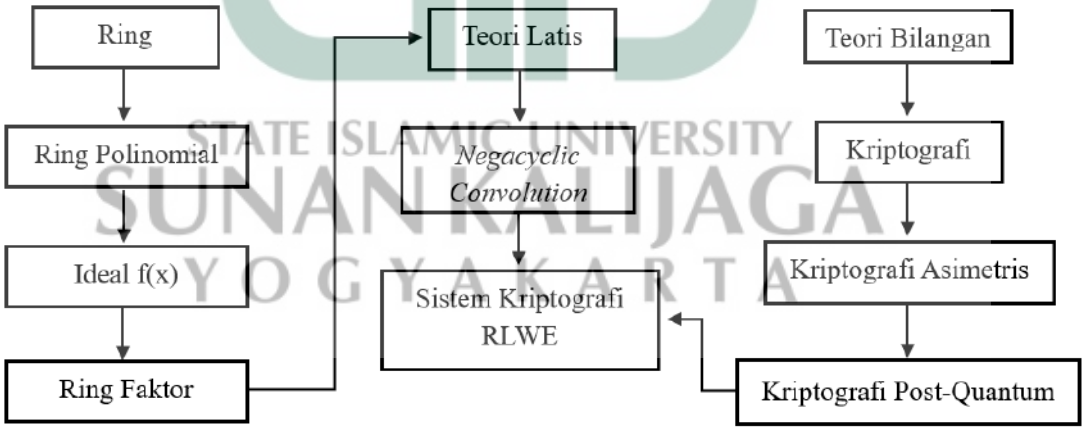
Pada penelitian ini digunakan metode penelitian berupa studi literatur, yakni pengkajian data dan informasi dari berbagai sumber ilmiah, seperti buku, artikel jurnal, prosiding, maupun publikasi *online* terkait. Pendekatan ini bertujuan untuk memahami lebih dalam mengenai konsep, teori, dan perkembangan terkait RLWE, mulai dari struktur matematis hingga sistem kriptografi.

Tahap awal penelitian dilakukan dengan pengkajian literatur-literatur utama, khususnya artikel Lyubashevsky et al. (2010) yang memperkenalkan pengembangan *Ring Learning with Errors* (RLWE). Untuk memahami transisi dari masalah LWE standar ke RLWE berbasis ring, dikaji pula literatur-literatur mengenai teori latis dan struktur aljabar yang mendasarinya. Selanjutnya dilakukan analisis terhadap konsep struktur aljabar yang membentuk RLWE. Secara umum, sistem kriptografi RLWE menggunakan konsep ring faktor atas ideal yang dibangun oleh suatu ring polinomial, khususnya ring faktor $R_q = \mathbb{Z}_q[x]/\langle f(x)\rangle$. Dalam hal ini, pengkajian dimulai dari pemilihan polinomial $f(x) = x^n + 1$ dengan n merupakan pangkat dari dua ($n = 2^k$). Polinomial tersebut dipilih karena memiliki sifat yang memungkinkan proses reduksi polinomial menjadi lebih sederhana dan efisien secara komputasi melalui $x^n \equiv -1 \pmod{x^4 + 1}$. Selain itu, dilakukan penentuan suatu parameter bilangan prima q yang memenuhi kriteria keamanan sistem dan memastikan operasi dalam ring faktor R_q dapat berjalan dengan stabil. Berikutnya dibahas pula struktur aljabar lain seperti sifat-sifat ring pada RLWE.

Selanjutnya, dilakukan pengkajian mekanisme kerja pada sistem kriptografi

yang meliputi tiga fungsi utama, yaitu tahap pembangkitan kunci (*key generation*), enkripsi, dan dekripsi. Pada pembangkitan kunci, diambil suatu elemen secara acak dari R_q untuk membentuk kunci publik (a, b). Kemudian pada proses enkripsi, dilakukan operasi biner dalam R_q dengan menambahkan *noise* e. Sementara itu, tahap dekripsi difokuskan pada manipulasi polinomial dan efektivitas penggunaan kunci rahasia untuk mengeliminasi pengaruh *noise* melalui teknik pembulatan koefisien.

Untuk pemahaman lebih lanjut, diberikan contoh implementasi sederhana melalui dua pendekatan, yakni perhitungan manual dan komputasi. Perhitungan manual untuk menunjukkan langkah-langkah algoritma skema kriptografi RLWE lebih detail, sehingga dapat lebih mudah dipahami. Sementara itu, pada bagian komputasi digunakan perangkat lunak SageMath 10.7. Contoh sederhana ini bertujuan untuk memastikan bahwa pesan yang didekripsi identik dengan pesan asli. Adapun alur atau skema penelitian dapat ditinjau pada Gambar 1.1 berikut.



Gambar 1.1 Skema Penelitian

1.8. Sistematika Penulisan

Penulisan tugas akhir ini disusun dengan sistematika sebagai berikut.

BAB I : Pada bab ini, dibahas mengenai latar belakang masalah, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, tinjauan pustaka dari penelitian terdahulu, metode penelitian, dan sistematika penelitian.

BAB II : Pada bab ini, dipaparkan teori-teori dasar yang mendukung pembahasan, meliputi konsep dasar ring, sejarah dan konsep kriptografi, serta konsep kongruensi dan algoritma pembagian.

BAB III : Pada bab ini, dipaparkan inti dari kajian teoretis dengan membahas konsep dasar RLWE, mekanisme sistem kriptografi kunci publik di RLWE, struktur aljabar yang terlibat, serta penggunaan konvolusi untuk efisiensi komputasi.

BAB IV : Pada bab ini disajikan contoh implementasi sederhana dari teori yang telah dibahas melalui simulasi manual dan simulasi komputasi menggunakan perangkat lunak SageMath. Contoh ini mencakup seluruh proses, mulai dari pembangkitan kunci hingga pesan dapat berhasil didekripsi kembali.

BAB V : Pada bab ini, dipaparkan kesimpulan yang diperoleh melalui hasil penelitian, serta saran-saran untuk pengembangan pada penelitian selanjutnya.

BAB V

PENUTUP

5.1. Kesimpulan

Berdasarkan studi literatur dan pengkajian yang telah dilakukan mengenai sistem kriptografi kunci publik pada RLWE, dapat diambil kesimpulan berikut.

1. Konsep yang melandasi ring $R_q = \mathbb{Z}_q[x]/\langle x^n + 1\rangle$, yaitu struktur ring faktor yang dibentuk atas ring polinomial $\mathbb{Z}_q[x]$ terhadap ideal utama yang dibangun oleh polinomial pembagi $f(x) = x^n + 1$. Melalui pemilahan derajat n sebagai pangkat dari dua ($n = 2^k$), memungkinkan setiap elemen direpresentasikan sebagai polinomial berderajat maksimal $n - 1$ dengan koefisien di $\mathbb{Z}_q$. Selain itu, pemilihan polinomial $x^n + 1$ dapat memanfaatkan sifat reduksi polinomial $x^n \equiv -1 \pmod{q}$, sehingga perkalian polinomial menjadi lebih sederhana dan efisien terutama secara komputasi.
2. Mekanisme sistem kriptografi kunci publik RLWE terdiri tiga tahap utama yang memanfaatkan *noise* sebagai dasar keamanannya, meliputi berikut.
    a. Pembangkitan kunci, Bob dapat menghasilkan pasangan kunci dengan memilih kunci rahasia $s(x)$ berkoefisien "kecil", lalu menghitung kunci publik $(a(x), b(x))$ dengan $b(x) = a(x)s(x) + e(x)$.
    b. Enkripsi, Alice menyandikan pesan menjadi suatu pasangan *ciphertext* $c = (v(x), w(x))$ dengan melibatkan kunci publik Bob dan penambahan *noise* baru untuk mengamankan pesan.

c. Dekripsi, Bob memulihkan pesan asli menggunakan kunci rahasia $s(x)$ untuk mengeliminasi atau menghapus kembali pengaruh *noise* melalui operasi polinomial dan teknik pembulatan koefisien.

3. Implementasi sistem kriptografi kunci publik RLWE dapat dilakukan dengan praktis melalui perangkat lunak SageMath. Proses ini mencakup penyusunan fungsi untuk mengonversi pesan menjadi representasi biner yang dipetakan ke dalam elemen-elemen ring R_q. Hasil dari implementasi menunjukkan bahwa seluruh tahapan, yakni mulai dari pembangkitan kunci hingga dekripsi dapat berjalan dengan sesuai. Pesan asli berhasil dipulihkan secara utuh.

5.2. Saran

Berdasarkan penelitian yang telah dilakukan, terdapat beberapa hal yang disarankan untuk dikembangkan dalam penelitian serupa selanjutnya, di antaranya:

1. Pengkajian lebih lanjut menggunakan NTT (*Number Theoretic Transform*).
2. Perlu dilakukan kajian lebih lanjut mengenai penggunaan jenis distribusi lain dalam pemilihan koefisien kunci rahasia dan *error*, seperti distribusi Gaussian yang lebih kompleks untuk membandingkan tingkat keberhasilan dekripsi.
3. Pengembangan implementasi dengan bahasa pemrograman yang lebih luas.

DAFTAR PUSTAKA

Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2015). Post-quantum key exchange - a new hope. Cryptology ePrint Archive, Paper 2015/1092, https://eprint.iacr.org/2015/1092.

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Biswas, R., Bolxo, S., Brandao, F. G. S. L., Buell, D. A., Burkett, B., Chen, Y., Chen, Z., Chlaro, B., Collins, R., Courtney, W., Dunsworth, A., Fahrl, E., Foxen, B., ..., & Martins, J. M. (2019). Quantum Supremacy Using a Programmable Superconducting Processor. *Nature*, 574:505–510, DOI: https://doi.org/10.1038/s41586-019-1666-5.

Baso, F. & Anriani, N. (2024). Implementasi teknik kriptografi dengan metode aes 256 untuk keamanan file. *INTEC Journal: Information Technology Education Journal*, 3(3):84–87.

Bossuat, J.-P., Cammarota, R., Chillotti, I., Curtis, B., Dai, W., Gong, H., Hales, E., Kim, D., Kumara, B., Lee, C., Lu, X., Maple, C., Pedrouzo-Ulloa, A., Player, R., Polyakov, Y., Ruiz Lopez, Luis Antonio, Song, Y., & Yhee, D. (2025). Security Guidelines for Implementing Homomorphic Encryption. Workingpaper, IACR Communications in Cryptology, DOI: 10.62056/anxra69p1.

Chacón, I. B. (2020). Ring learning with errors: A crossroads between postquantum cryptography, machine learning and number theory. https://arxiv.org/abs/1902.08551.

Chandra (2016). Keamanan data dengan metode kriptografi kunci publik. *Jurnal TIMES*, 5(2):11–15, ISSN: 2337-3601.

Cynthia, M. M., Cynthia, E. P., & Cynthia, D. N. (2026). Perbandingan algoritma kriptografi modern dalam melindungi data transmisi. *Jurnal Ilmu Komputer dan Teknik Informatika*, 2(1):29–35, DOI: 10.64803.

de Boer, K. & van Woerden, W. (2025). Lattice-based Cryptography: A survey on the security of the lattice-based NIST finalists. Cryptology ePrint Archive, Paper 2025/304, https://eprint.iacr.org/2025/304.

Dizon, M. A. C. & Meehan, A. (2025). Technical principles and protocols of encryption and their significance and effects on technology regulation. *Information & Communications Technology Law*, 34(2):79–105, DOI: 10.1080/13600834.2024.2404280, https://doi.org/10.1080/13600834.2024.2404280.

Douglas, R. S. & Paterson, M. B. (2019). *Cryptography Theory and Practice*. CRC Press, ISBN: 978-1-1381-9701-5.

Ducas, L. & Durmus, A. (2012). Ring-LWE in Polynomial Rings. Cryptology ePrint Archive, Paper 2012/235, https://eprint.iacr.org/2012/235.

Dummit, D. S. & Foote, R. M. (2004). *Abstract Algebra Third Edition*. John Wiley & Sons, Inc.

Ferdose, A. (2019). Cryptography: Principles, Techniques, and Applications. *International Journal of Innovative Research in Technology*, 5(8), ISSN: 2349-6002.

Hoffstein, J., Silverman, J. H., & Pipher, J. (2008). *An Introduction to Mathematical Cryptography*. Springer New York, DOI: https://doi.org/10.1007/978-0-387-77993-5.

International Business Machines Corporation (IBM) (2024). Cybersecurity trends: Ibm's predictions for 2025. https://www.ibm.com/think/insights/cybersecurity-trends-ibm-predictions-2025.

International Business Machines Corporation (IBM) (2025). Cybersecurity trends: Ibm's predictions for 2026. https://www.ibm.com/think/news/cybersecurity-trends-predictions-2026.

Kumar, M. (2022). Post-quantum cryptography Algorithm's standardization and performance analysis. *Array*, 15:100242, ISSN: 2590-0056, DOI: https://doi.org/10.1016/j.array.2022.100242, https://www.sciencedirect.com/science/article/pii/S2590005622000777.

Lindner, R. & Peikert, C. (2011). Better key sizes (and attacks) for lwe-based encryption. In Kiayias, A., editor, *Topics in Cryptology – CT-RSA 2011*, pages 319–339, Berlin, Heidelberg. Springer Berlin Heidelberg, ISBN: 978-3-642-19074-2.

Lyubashevsky, V., Peikert, C., & Regev, O. (2010). On ideal lattices and learning with errors over rings. In Gilbert, H., editor, *Advances in Cryptology – EUROCRYPT 2010*, pages 1–23, Berlin, Heidelberg. Springer Berlin Heidelberg, ISBN: 978-3-642-13190-5.

Malik, D. S., Mordeson, J. M., & Sen, M. K. (1997). *Fundamentals of Abstract Algebra*. The McGraw-Hill Companies, Inc, ISBN: 978-0-321-50031-1.

Mohan, R., Sah, P. K., Raj, A. M., & Sah, A. K. (2025). Evolution of cryptographic techniques: From ancient ciphers to modern encryption systems. *IOSR Journal of Mathematics (IOSR-JM)*, 21(3):12–19.

Nwaga, P. C. & Nwagwughiagwu, S. (2024). Exploring the significance of quantum cryptography in future network seccurity protocols. *World Journal of Advanced Research and Reviews (WJARR)*, 24(3):817–833, DOI: 10.30574.

Peikert, C. (2016). A Decade of Lattice Cryptography. *Foundations and Trends in Theoretical Computer Science*, 10(4):283–424, ISSN: 1551-305X, DOI: 10.1561/0400000074, https://doi.org/10.1561/0400000074.

Regev, O. (2010). The learning with errors problem (invited survey). In *2010 IEEE 25th Annual Conference on Computational Complexity*. DOI: 10.1109/CCC.2010.26.

Roos, S. & Jung, M. (2020). *An Introductory Course on Sage*. University of Postdam.

Rosen, b. K. (2011). *Elementary Number Theory and Its Applications*. pearson highered.

Scrivano, A. (2025). A Comparative Study of Classical and Post-Quantum Cryptographic Algorithms in the Era of Quantum Computing. *Arxiv*, abs/2508.00832, DOI: https://doi.org/10.48550/arXiv.2508.00832, https://arxiv.org/abs/2508.00832.

Sengupta, B., Gupta, P., & Sengupta, S. (2025). Introduction to Number Theoretic Transform. https://arxiv.org/abs/2509.05884.

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. https://cc.ee.ntu.edu.tw/~rbwu/rapid_content/course/QC/Shor1994.pdf.

Simarmata, J., Sriadhi, & Rahim, R. (2019). *Kriptografi Keamanan Data & Informasi*. Penerbit ANDI, Anggota IKAPI, Medan.

Sitohang, H., Saing, R. U. P., Sarahono, A. S. O., Purba, J. S., Tebai, P., & Hasugian, P. M. (2024). Cryptography with the Ring-LWE (Learning With Errors) Algorithm. *Ju Ti: Indonesian Engineering Journal*, 3(1):30–35, ISSN: 2964-0490.

Opiłka, Filip, Niemiec, M., Gagliardi, M., & Kourtis, M. A. (2024). Performanse Analysis of Post-Quantum Cryptography Algorithms for Digital Signature. *Applied Sciences*, 14(12), DOI: https://doi.org/10.3390/app14124994.

Thawte.inc (2013). History of cryptography. adgrafics.net, https://adgrafics.net/docs/thawte/history-cryptography.pdf. Diakses pada: 02-26.

The Sage Development Team (2025). *History and License Release 10.8*. sagemath.org.

Wahyuni, S., Wijayanti, I. E., Yuwaningsih, D. A., & Hartanto, A. D. (2016). *Teori Ring dan Modul*. Gadjah Mada University Press, ISBN: 978-602-386-118-7.

Wohlwend, J. (2016). Elliptic curve cryptography: Pre and post quantum. MIT Mathematics, https://math.mit.edu/~apost/courses/18.204-2016/18.204_Jeremy_Wohlwend_final_paper.pdf. Diakses pada: 06-02-26.

Zimmermann, P., Casamayou, A., Cohen, N., Connan, G., Dumont, T., Fousse, L., Maltey, F., Meulien, M., Mezzarobba, M., Pernet, C., Thiéry, N. M., Bray, E., Cremona, J., Forets, M., Ghitza, A., & Thomas, H. (2018). *Computational Mathematics with SageMath*. Society for Industrial and Applied Mathematics, Philadelphia, PA, DOI: 10.1137/1.9781611975468, https://epubs.siam.org/doi/abs/10.1137/1.9781611975468.