BAB I

PENDAHULUAN

1.1 Latar Belakang

Kriptografi menjadi salah satu pendekatan yang banyak digunakan karena mampu memberikan perlindungan terhadap ancaman keamanan dalam komunikasi digital. Menurut (Setiawan, 2025), kriptografi bekerja dengan cara melakukan proses enkripsi, yaitu mengubah data menjadi bentuk yang tidak dapat dibaca tanpa kunci tertentu. Salah satu kategori utama kriptografi adalah kriptografi klasik, yang prinsip kerjanya dijelaskan oleh (Yu, 2023). Beberapa algoritma yang termasuk ke dalam kategori kriptografi klasik antara lain Rivest-Shamir-Adleman (RSA), digunakan untuk mengubah sebuah kalimat menjadi tidak dapat dimengerti dalam bentuk hexadesimal 32 hingga 64 bytes (Dzahabi et al., 2025), dan algoritma *Advanced Encryption Standard* (AES), digunakan untuk melakukan enkripsi pada file teks (Latip, 2025).

National Institute of Standards and Technology (NIST) telah melakukan proses standarisasi terhadap berbagai algoritma kriptografi klasik baru sebagai bentuk adaptasi terhadap kebutuhan keamanan masa kini (Alagic et al., 2022, 2024, 2025; Moody et al., 2020). Salah satu jenis algoritma yang terpilih meliputi algoritma berbasis kisi seperti *Nth Degree Truncated Polynomial* (NTRU), yang pada penelitian (Purba et al., 2019) digunakan untuk pengamanan data teks, serta Kyber, yang digunakan untuk melakukan pertukaran kunci (Xing et al., 2021). (Scrivano, 2025) menegaskan bahwa langkah standarisasi tersebut diperlukan untuk menyesuaikan diri dengan perkembangan teknologi dan sebagai alternatif jika

algoritma klasik yang telah lama digunakan menjadi tidak relevan di masa mendatang.

Algoritma kriptografi berbasis kisi seperti NTRU digunakan karena termasuk dalam kategori kriptografi klasik yang memiliki basis perhitungan lebih rumit, karena memiliki perhitungan matematis yang lebih kompleks dibandingkan dengan metode berbasis faktorisasi bilangan bulat dan logaritma diskrit seperti pada RSA (Ranasinghe et al., 2024) (Nguyen et al., 2025). (Eid et al., 2025) menjelaskan bahwa algoritma berbasis kisi memanfaatkan himpunan titik-titik dalam ruang berdimensi tinggi yang dibentuk dari kombinasi linear vektor dengan koefisien bilangan bulat. Dalam konteks algoritma NTRU, (Boer et al., 2025) menjelaskan bahwa struktur matematis tersebut diimplementasikan dalam bentuk *ring* polinomial $R = \mathbb{Z}_q[x]/(x^n - 1)$, seluruh operasi dilakukan terhadap polinomial dengan koefesien modulo q, dan hasil dikembalikan ke derajat dibawah n melalui reduksi terhadap $(x^n - 1)$.

Penelitian terkait NTRU terus dikembangkan untuk meningkatkan kecepatan komputasi, (Zhou et al., 2018) mengusulkan metode untuk mempercepat proses perhitungan agar kompleksitas waktu komputasi dapat dikurangi dari $O(n^2)$. Sementara itu, (Liu et al., 2025) menekankan pentingnya optimalisasi waktu dalam proses pembangkitan kunci, enkripsi, dan dekripsi pada algoritma NTRU. Menurut (An et al., 2018), kinerja algoritma NTRU sangat dipengaruhi oleh penentuan tiga parameter utama, yaitu n, q, dan p; yang berarti n menunjukkan derajat polinomial dalam *ring* $R = \mathbb{Z}_q[x]/(x^n - 1)$ yang berpengaruh terhadap dimensi kisi; parameter q berfungsi sebagai modulus besar dalam operasi aritmetika pada ring

tersebut, di mana semua koefisien polinomial direduksi terhadap nilai q; sementara parameter p digunakan untuk reduksi hasil perkalian polinomial sebelum proses dekripsi dilakukan, nilai q yang besar akan meningkatkan panjang bit dari setiap koefisien, sehingga berdampak pada bertambahnya ukuran kunci dan ciphertext.

Upaya untuk memodifikasi parameter telah menjadi fokus berbagai penelitian lanjutan, seperti penelitian (Zhou et al., 2018), yang memperkenalkan teknik *preprocess-then NTT* untuk mengurangi batasan modulus q, sehingga tidak lagi mensyaratkan $q \equiv 1 \pmod{2n}$ dan cukup $q \equiv 1 \pmod{n}$ pada *1-round PtNTT* atau $q \equiv 1 \pmod{n/2}$ pada *2-round PtNTT*. Selanjutnya, (Zhu et al., 2019) mengembangkan pendekatan hibrid Karatsuba–NTT yang memungkinkan penurunan nilai q tanpa mengurangi kinerja proses perhitungan. Penelitian tersebut kemudian disempurnakan oleh (Kundu et al., 2022), yang memperbaiki kesalahan dalam formula hibrid NTT–Karatsuba milik (Zhu et al., 2019), dan membuktikan kebenaran matematisnya melalui teknik pemisahan 2^{α} (*2-alpha-part separation*). Hasil penelitian tersebut menunjukkan bahwa nilai parameter q dapat dikompresi secara signifikan, yakni dari 1061093377 menjadi 83969 untuk $n = 1024$, dan dari $2^{57} + 25 \cdot 2^{13} + 1$ menjadi 166657 untuk $n = 2048$.

Penelitian terdahulu (Zhou et al., 2018)(Zhu et al., 2019) (Kundu et al., 2022) berupaya untuk melakukan kompresi nilai parameter modulus besar q yang sangat berpengaruh dalam menentukan besaran ukuran kunci dan *ciphertext*. Apabila nilai parameter q terlalu besar, maka ukuran kunci dan ciphertext juga besar, hal tersebut dapat mengakibatkan penggunaan bandwidth yang besar sehingga biaya komputasi menjadi mahal. Selain melakukan kompresi pada parameter q, penelitian terhadap

proses perkalian polinomial juga dilakukan. Hal tersebut bertujuan untuk mencari metode perhitungan yang dapat mempercepat proses perkalian polinomial sehingga kompleksitas waktu komputasi bisa mendekati atau sampai dengan $O(n \log n)$ yang dapat menambah kecepatan proses kerja dari algoritma kriptografi yang digunakan. Berbeda dari (Zhou et al., 2018) yang hanya menggunakan NTT, penelitian (Zhu et al., 2019)(Kundu et al., 2022) menggunakan pendekatan hibrid untuk mengoptimalkan perkalian polinomial menggunakan Karatsuba karena terdapat beberapa keterbatasan berdasarkan parameternya. Karatsuba menangani perkalian polinomial berderajat kurang dari 768, keterbatasan tersebut dapat diatasi dengan menggunakan pendekatan hibrid. Saat melakukan perkalian polinomial menggunakan NTT, dapat diketahui bahwa perkaliannya $h = f \cdot g = NTT^{-1}\ (NTT(F\ )$ □ $q\ NTT(G))$. Lalu, apabila dilakukan hibrid dengan Karatsuba hanya perlu menemukan NTT^{-1} dari NTT untuk perkalian polinomial primer $f0, f1, g0, g1$, hal ini dapat mengurangi kompleksitas waktu algoritma. Karatsuba memecah polinomial berderajat besar menjadi kombinasi polinomial berderajat lebih kecil. Hal ini menyebabkan percepatan perkalian komponen demi komponen NTT setelah teknik hibrid diterapkan.

Meskipun berbagai penelitian sebelumnya telah membahas kompresi parameter q dan optimasi perkalian polinomial, masih terdapat beberapa kekurangan yang belum dijawab secara menyeluruh. Hingga kini, belum adanya penelitian yang menguji implementasi nyata dari pendekatan hibrid NTT–Karatsuba langsung pada proses kerja lengkap algoritma NTRU, mulai dari key generation, enkripsi, hingga dekripsi. Selain itu, kurangnya analisis mengenai

dampak kompresi modulus q terhadap ukuran kunci, ciphertext, dan penggunaan bandwidth membuat dampak kompresi belum dapat dinilai secara objektif. Di sisi lain, tidak adanya pengukuran tingkat bit keamanan untuk parameter yang digunakan dalam skema algoritma menyebabkan tingkat keamanan belum dapat dipastikan.

Berdasarkan kekurangan tersebut, penelitian ini bertujuan untuk menguji performa dari hasil perhitungan matematis hibrid NTT-Karatsuba dengan mengimplementasikannya kedalam proses kerja algoritma NTRU meliputi pembangkitan kunci, enkripsi, dan dekripsi, yang pada akhirnya dilakukan proses analisis apabila terdapat kegagalan dekripsi. Lalu, hasil dari kompresi parameter q akan diukur untuk melihat seberapa besar pengaruhnya terhadap penurunan ukuran kunci dan *ciphertext* pada proses sebelum dan sesudah dilakukannya kompresi. Selain ukuran kunci dan ciphertext, penggunaan bandwidth juga akan dilakukan pengukuran untuk melihat penurunan nilai penggunaan bandwidth dari sebelum dan sesudah dilakukannya kompresi parameter q. Terakhir, penelitian ini mengukur performa tingkat bit keamanan dari parameter hasil kompresi, yang dilakukan untuk mengetahui berapa lama proses komputasi yang dibutuhkan untuk memecahkan skema algoritma NTRU yang digunakan.

1.2 Rumusan Masalah

Berdasarkan penjelasan latar belakang, maka rumusan masalah penelitian ini adalah:

a. Bagaimana pengaruh metode Number theoretic transform dengan Karatsuba dalam kecepatan proses perhitungan perkalian polinomial?

b. Bagaimana pengaruh kompresi parameter modulus besar (q) terhadap nilai bit keamanan algoritma NTRU?
c. Bagaimana pengaruh kompresi modulus besar (q) terhadap ukuran kunci publik dan ciphertext?
d. Bagaimana pengaruh kompresi modulus besar (q) terhadap nilai besaran bandwidth yang digunakan?
e. Bagaimana pengaruh hasil kompresi ukuran kunci publik dan ciphertext terhadap nilai kompleksitas waktu proses keygen, enkripsi dan dekripsi?

1.3 Tujuan Penelitian

Berdasarkan penjelasan pada rumusan masalah, tujuan dari penelitian ini adalah:

a. Mengukur waktu kecepatan proses perhitungan polinomial menggunakan metode Number Theoritic Transform dengan Karatsuba.
b. Mengukur tingkat bit keamanan berdasarkan pengaruh kompresi parameter modulus besar (q) terhadap algoritma NTRU.
c. Mengukur pengaruh kompresi modulus besar (q) terhadap perubahan ukuran kunci publik dan ciphertext yang dihasilkan oleh algoritma NTRU.
d. Mengukur perbedaan penggunaan bandwidth antara parameter sebelum dan sesudah kompresi modulus besar (q).
e. Mengukur pengaruh perubahan ukuran kunci publik dan ciphertext pada algoritma NTRU terhadap waktu proses *key generation*, enkripsi, dan dekripsi.

1.4 Manfaat Penelitian

Adapun manfaat yang bisa didapatkan dari penelitian ini adalah:

a. Memberikan kontribusi dalam pengembangan ilmu pengetahuan di bidang kriptografi pasca-kuantum, khususnya terkait penerapan metode Hybridized NTT-Karatsuba pada algoritma NTRU.
b. Menjadi referensi bagi peneliti dan praktisi dalam memahami tantangan dan peluang yang dihadapi untuk pengembangan parameter algoritma NTRU.
c. Menjadi referensi akademis mengenai efektivitas kompresi parameter dalam memengaruhi waktu komputasi serta ukuran kunci dan ciphertext pada skema kriptografi berbasis NTRU.
d. Menambah literatur penelitian mengenai optimasi perhitungan polinomial untuk memperbaiki performa algoritma kriptografi berbasis *lattice*.

1.5 Batasan Masalah

Batasan masalah dalam penelitian ini adalah:

a. Algoritma yang digunakan terbatas pada NTRU dengan penerapan metode hibrid NTT-Karatsuba.
b. Parameter yang diuji difokuskan pada parameter hasil kompresi meliputi n=1024, q=83969 dan n=2048, q=166657.
c. Metode evaluasi hanya mencakup pengukuran performa tingkat keamanan yang dihasilkan, waktu komputasi untuk proses perkalian polinomial, waktu komputasi proses keygen, enkripsi, dan dekripsi, analisis ukuran kunci dan ciphertext, besaran bandwidth yang digunakan, dan kegagalan hasil dekripsi.
d. Penelitian ini tidak membahas aspek integrasi ke dalam protokol komunikasi penuh seperti TLS/SSL, tetapi hanya fokus pada algoritma NTRU.