SKRIPSI

SISTEM KRIPTOGRAFI *NTRU* PADA PROSES PENGAMANAN DATA RAHASIA

YULIA FATIN LESTARI

16610033

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2021

SISTEM KRIPTOGRAFI *NTRU* PADA PROSES PENGAMANAN DATA RAHASIA

Skripsi

Untuk memenuhi sebagian persyaratan

mencapai derajat Sarjana S-1

Program Studi Matematika

diajukan oleh

YULIA FATIN LESTARI

16610033

Kepada

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2021

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi / Tugas Akhir
Lamp :

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 : Yulia Fatin Lestari
NIM : 16610033
Judul Skripsi : Sistem Kriptografi NTRU Pada Proses Pengamanan Data Rahasia

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 dimunaqsyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 16 April 2021
Pembimbing

Muhammad 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-740/Un.02/DST/PP.00.9/05/2021

Tugas Akhir dengan judul : SISTEM KRIPTOGRAFI NTRU PADA PROSES PENGAMANAN DATA RAHASIA

yang dipersiapkan dan disusun oleh:

Nama : YULIA FATIN LESTARI
Nomor Induk Mahasiswa : 16610033
Telah diujikan pada : Senin, 26 April 2021
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: 60b1b3a42800c

Penguji I

Dr. Muhammad Wakhid Musthofa, S.Si., M.Si.
SIGNED

Valid ID: 60b0675b2c766

Penguji II

Sri Istiyarti Uswatun Chasanah, M.Si.
SIGNED

Valid ID: 60b1b4289ceca

Yogyakarta, 26 April 2021
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

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

Valid ID: 60b74a1445919

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini:

Nama	: Yulia Fatin Lestari
NIM	: 16610033
Program Studi	: Matematika
Fakultas	: Sains dan Teknologi

Dengan ini menyatakan bahwa isi 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, 16 April 2021

Yang Menyatakan

Yulia Fatin Lestari

Karya sederhana ini penulis persembahkan

untuk keluarga tercinta yang senantiasa memotivasi

dalam segala kondisi

"Kami telah turunkan kepadamu Al-Dzikir (Al-Quran) untuk kamu terangkan kepada manusia apa-apa yang diturunkan kepada mereka agar mereka berpikir"

(QS. 16:44)

PRAKATA

Assalamualaikum Wr. Wb. Alhamdulillah, segala puji bagi Allah SWT yang telah memberikan nikmat, kesehatan serta kesempatan sehingga penulis dapat menyelesaikan skripsi dengan judul Sistem Kriptografi NTRU pada Proses Pengamanan Data Rahasia. Skripsi ini merupakan salah satu syarat untuk memperoleh gelar sarjana program studi Matematika di Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Dalam proses penulisan skripsi ini tidak terlepas dari dukungan dan bimbingan dari berbagai pihak. Oleh karena itu, penulis mengucapkan rasa terima kasih kepada:

1. Dr. Khurul Wardati, S.Si, M.Si selaku Dekan Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.
2. Muchammad Abrori, S.Si, M.Kom selaku Ketua Program Studi Matematika.
3. Dr. Epha Diana Supandi, S.Si, M.Sc selaku Dosen Penasehat Akademik Matematika 2016 yang senantiasa mengayomi.
4. Muhammad Zaki Riyanto, S.Si, M.Sc selaku Dosen Pembimbing Skripsi telah memberikan bimbingan dan arahan dalam penyusunan Skripsi hingga selesai.
5. Bapak dan Ibu dosen Program Studi Matematika yang telah memberi bekal ilmu pengetahuan selama perkuliahan.
6. Ibu (Suharti) dan Bapak (Sugiman), serta kakak (Septianingsih) yang senantiasa mendo'akan serta memberikan dukungan kepada penulis sehingga mam-

pu menyelesaikan skripsi.

7. Keluarga besar Matematika 2016 yang telah mewarnai hari-hari penulis selama masa perkuliahan.
8. Teman-teman yang selalu ada membersamai saat tangis dan tawa yaitu Cindyana, Fitrin, Martingsih, Riska, Salsabila, Sherlin.
9. Keluarga KKN Konservasi Kendal yaitu Bahaul, Dafa, Fikri, Irsyad, Nurul, Sherlin, Sri, Udin, dan Ulfa.
10. Rekan seperjuangan aljabar Yunida, Fadly, Nenti, dan Yenni yang senantiasa menyemangati penulis untuk menyelesaikan skripsi ini.

Penulis menyadari masih banyak kekurangan dalam penyusunan skripsi ini, untuk itu diharapkan saran dan kritik yang bersifat membangun demi kesempurnaan penulisan skripsi ini. Namun demikian, penulis tetap berharap semoga skripsi ini dapat bermanfaat dalam perkembangan ilmu matematika dan siapapun yang membacanya. Wassalamualaikum Wr. Wb.

Yogyakarta, 8 Maret 2021

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR LAMBANG

R	: Ring
$a \in R$	: a anggota R
e	: elemen identitas
$\mathbb{Z}$	: himpunan bilangan bulat
$R[x]$	: ring polinomial
R/I	: ring faktor
$\deg f(x)$	: derajat polinomial $f(x)$
$\langle a \rangle$	: Ideal yang dibangun oleh a
$\phi(x)$	: elemen identitas suatu polinomial
$\psi(x)$	: elemen invers suatu polinomial
$\sum_{i=1}^{n} a_i$	: penjumlahan $a_1 + a_2 + \cdots + a_n$
I	: ideal
$a\|b$	: a membagi habis b
$I \subseteq R$	: I himpunan bagian atau sama dengan R.

INTISARI

SISTEM KRIPTOGRAFI *NTRU* PADA PROSES PENGAMANAN DATA RAHASIA

Oleh

YULIA FATIN LESTARI

16610033

NTRU merupakan salah satu sistem kriptografi asimetris yang pertama kali diperkenalkan oleh Jeffrey Hoffstein, Jill Pipher dan Joseph Silverman pada tahun 1996. Sistem kriptografi NTRU diangggap lebih aman dalam menghadapi komputer quantum.

Proses yang dilakukan pada NTRU menggunakan ring polinomial. Enkripsi dan dekripsi dari sistem kriptografi NTRU menggunakan ring faktor atas ideal yang dibangun oleh elemen di ring polinomial, seperti $R = \mathbb{Z}[x]/(x^N - 1)$. Diberikan ring $\mathbb{Z}$ merupakan ring komutatif dengan elemen satuan, maka dapat dibentuk suatu ring polinomial $\mathbb{Z}[x]$. Misal $g(x)$ merupakan polinomial irredusibel berderajat N di $\mathbb{Z}$, maka ring faktor $\mathbb{Z}[x]/(x^N - 1)$ yang terbentuk ring komutatif dengan elemen satuan berderajat $n - 1$. Perhitungan pada sistem kriptografi NTRU dilakukan menggunakan SageMath.

Kata kunci : enkripsi, kriptografi, NTRU, ring polinomial

ABSTRACT

By

YULIA FATIN LESTARI

16610033

NTRU is one of the asymmetric cryptosystems first introduced by Jeffrey Hoffstein, Jill Pipher and Joseph Silverman in 1996. The NTRU cryptosystem is considered to be more secure in dealing with quantum computers.

NTRU uses a polynomial ring. The encryption and decryption of the NTRU cryptosystem usess ideal over ring factor constructed by elements in the polynomial ring, such as $R = \mathbb{Z}[x]/(x^N - 1)$. Given $\mathbb{Z}$ is a commutative ring with unit elements, a polynomial $mathbbZ[x]$ can be formed. Given $g(x)$ is an irreducible polynomial with degree N in $mathbbZ[x]$, then the quotien rings $\mathbb{Z}[x]/(x^N - 1)$ is formed as a commutative ring with unit elements of degree $n - 1$. NTRU cryptosystem in this research are coded using SageMath.

Keyword : encryption, cryptography, NTRU, polynomial ring.

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Manusia diciptakan oleh Allah sebagai makhluk sosial, sehingga dalam kehidupan sehari-hari dibutuhkah interaksi antar manusia. Oleh karena itu komunikasi merupakan kebutuhan yang penting dalam berlangsungnya kehidupan dengan tujuan bertukar informasi. Sebagaimana yang dijelaskan dalam Al-Qur'an surat Ar-rahman ayat 1-4,

Artinya:

Allah Yang Maha Pengasih, Yang telah mengajaarkan Al-Qur'an. Dia menciptakan manusia, mengajarnya pandai berbicara.

Potongan ayat seperti di atas memperlihatkan bahwa Allah telah memberi kemampuan kepada umatnya untuk berbicara (komunikasi). Tujuan dari komunikasi adalah agar dapat saling memberi kabar antara satu dengan lainnya. Pada masa sebelumnya manusia berkomunikasi menggunakan tulisan dan lisan. Namun pada era digital seperti sekarang dimana perkembangan teknologi semakin canggih, manusia dapat berkomunikasi menggunakan telepon seluler dan komputer. Salah satu jalur yang digunakan saat ini adalah jalur komunikasi internet.

Kebutuhan akses komunikasi-informasi yang mudah dan murah, sehingga

internet merupakan salah satu solusi. Internet merupakan jaringan yang terdiri dari jutaan komputer yang terhubung antara satu dan yang lainya dengan pemanfaatan jaringan telepon baik berupa kabel maupun gelombang elektromagnetik, sehingga internet terhubung secara internasional dan tersebar diseluruh dunia. Hal ini menyebabkan semua orang dapat menggunakan jalur komunikasi internet secara bebas tak terbatas. Bahkan orang yang tidak berhak dapat mengaksesnya.

Semakin banyak orang yang mengakses mengakibatkan internet menjadi jalur komunikasi yang tidak aman. Informasi-informasi rahasia yang dikirimkan melalui jalur yang tidak aman memudahkan pihak ketiga untuk memperoleh informasi tersebut dan digunakan untuk melakukan hal negatif. Dibutuhkan solusi untuk mengamankan informasi tersebut agar tidak diketahui oleh pihak ketiga.

Kriptografi merupakan solusi untuk mengatasi permasalahn informasi. Kriptologi merupakan suatu ilmu yang memepelajari tentang kode rahasia. Digunakan dalam bidang politik dan bidang militer sejak abad pertengahan sampai abad 20. Terdapat dua hal penting yang dipelajari pada kriptologi yaitu kriptografi dan kriptanalisis. Kriptografi atau disebut juga dengan sandi *cipher* merupakan fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Tujuan utama kriptografi adalah untuk mengamankan informasi rahasia melalui saluran yang tidak aman seperti internet.

Kriptanalisis adalah teknik matematika untuk mencoba memcahkan teknik kriptografi dan keamanan informasi. Mempelari kelemahan suatu sistem dengan begitu dapat diketahui cara untuk membuatnya menjadi sistem yang lebih kuat. Kriptosistem yang baik dapat mempersulit perolehan informasi dari *ciphertext* menjadi *plaintext* tanpa mengetahui kunci. Hal tersebut juga harusnya mempersulit pihak ketiga yang ingin mencuri kunci rahasia.

Terdapat dua tipe sistem kriptografi yaitu: simetris dan asimetris. Sistem kriptografi simetris menggunakan kunci yang sama pada proses enkripsi dan dekripsi. Sedangkan kriptografi asimetris menggunakan sepasang kunci yang dibuat yaitu kunci publik dan kunci privat.

Pada tahun 1976 sistem kriptografi baru diusulkan oleh Martin Hellman dan Whitfield Diffie yang dikenal dengan kriptografi asimetris. Mereka memikirkan metode dimana kunci enkripsi berbeda dengan kunci dekripsi. Setelahnya banyak bermunculan algoritma kriptosistem baru seperti RSA, ElGamal, dan Kurva Eliptik. Ketiga algoritma tersebut sukses dan banyak digunakan dalam situasi yang berbeda. Dengan keberhasilan tersebut dirasa perlu menemukan algoritma pengganti yang cocok dengan dengan alasan sebgai berikut:

1. Suatu serangan yang vital merusak Algoritma-algoritma tersebut maka semua pengaplikasian yang berdasarkan ketiganya akan rusak.

2. Proses penghitungan yang sangat besar untuk dilakukan pada beberapa sistem dimana kemampuan perhitungan dan kapasitas tenaga yang dimiliki terbatas.

3. Kecepatan enkripsi dan dekripsi ketiga algoritma terbilang lamban begitu juga pembentukakn kuncinya.

Berdasarkan alasan seperti yang telah dipaparkan maka dicari kriptosistem yang baru dengan mempertimbangkan efisiensi dan membatasi resiko penyerangan berdasarkan faktorisasi dan logaritma diskrit. Hingga diajukannya algoritma NTRU, yaitu sistem kriptografi yang didasarkan ring polinomial, pada Crypto'96. NTRU beroperasi dalam ring $Z[x]/(X^N - 1)$.

1.2. Batasan Masalah

Pada suatu penelitian sangatlah penting adanya batasan masalah karena untuk menghindari meluasnya pembahasan yang tidak terarah terhadap objek penelitian, dengan adanya pembatasan masalah akan membatu peneliti memfokuskan pada objek yang dituju. Berdasarkan latar belakang yang telah dipaparkan, penelitian ini akan difokuskan pada pembahasan algoritma NTRU. Penelitian ini diawali dengan pembentukan kunci publik yang setelahnya akan diberikan contoh proses enkripi serta dekripsi pesan. Serta diberikna contokk kasus sistem kriptografi NTRU menggunakan SageMath.

1.3. Rumusan Masalah

Berdasarkan latar belakang dan batasan masalah yang telah dipaparkan, maka dapat dirumuskan beberapa permasalahan sebagai berikut:

1. Bagaimana peran struktur aljabar pada sistem kriptografi NTRU?
2. Bagaimana cara kerja sistem kriptografi NTRU dalam melakukan proses pembentukan kunci, enkripsi dan dekripsi serta contoh perhitungannya menggunakan SageMath?

1.4. Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Mengkaji secara matematis mengenai pembentukan ring $\mathcal{R} = \mathbb{Z}[x]/(x^N - 1)$.
2. Mengkaji tentang proses sistem kriptografi NTRU.

1.5. Manfaat Penelitian

Hasil dari penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Mengetahui struktur aljabar pada sistem kriptografi NTRU.
2. Mengetahui cara kerja sistem kriptografi NTRU dalam melakukan proses pembentukan kunci, enkripsi dan dekripsi.

1.6. Tinjauan Pustaka

Jurnal karya Ayushi, (2010) memaparkan tentang sistem kriptografi yang terbagi menjadi dua yaitu sistem kriptografi simetris dan kriptografi asimetris. Perbedaan keduanya terletak pada kunci yang digunakan jika pada sistem kriptografi simetris menggunakan kunci yang sama saat melakukakn enkripsi dan dekripsi sementara pada sistem kriptografi asimetris menggunakan kunci yang berbeda saat melakukan enkripsi dan dekripsi.

Kriptografi adalah suatu ilmu yang memepelajari teknik-teknik matematika yang berhungan dengan aspek informasi. Salah satunya adalah sistem kriptografi NTRU yang diperkenalkan pada tahun 1996 oleh J. H. Silverman, J. Hoffstein, dan Jill Piper. Sistem kriptografi NTRU dikontruksi menggunakan konsep ring faktor atas ideal yang dibangun oleh elemen di ring polinomial $\mathbb{Z}[x]$. Dimisalkan terdapat dua pihak yang akan bertukar pesan yaitu Alice dan Bob. Sistem tersebut Alice bertugas membuat kunci publik menggunakan rumus $h(x) = f^{-1}(x)g(x) \pmod q$, sebelumnya Alice telah memilih $F(x)$ dan $G(x)$. Menggunakan kunci publik yang telah dibuat oleh Alice, maka Bob dapat mengirim pesan dengan melakukan enkripsi menggunakan rumus $e_K(y) = r \times h + m \pmod q$. Untuk mengetahui pesan yang telah dikirim oleh Bob maka Alice melakukan proses dekripsi yaitu mengembalikan

pesan asli menggunakan rumus $d_K(y) = (f \times y \mod q) \mod p$. Materi tersebut dikembangkan oleh Paterson, M. B., dkk. (2019).

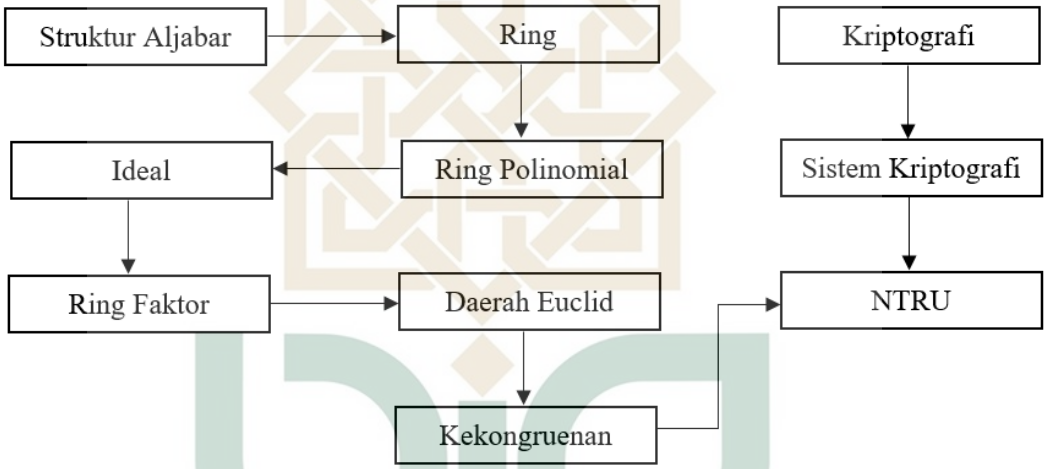
Penelitian ini akan membahas tentang sistem kriptografi NTRU. Keamanan sistem kriptografi NTRU menggunakan konsep ring faktor atas ideal yang dibangun oleh elemen di ring polinomial $\mathbb{Z}[x]$. Ring faktor yang digunakan berupa $\mathcal{R} = \mathbb{Z}[x]/(x^N - 1)$. Kontruksi ring tersebut merujuk pada buku yang ditulis oleh Malik, D. S., (1997) berisi teori-teori dasar aljabar. Selain itu digunakan juga buku pendukung karya Rosen, Kenneth (2011) yang membahas kongruensi.

1.7. Metode Penelitian

Metode yang digunakan adalah studi literatur, yaitu dengn mengambil data-data dan informasi dari buku dan jurnal matematika. Secara umum, sistem kriptografi NTRU menggunakan konsep ring faktor atas ideal yang dibangun oleh elemen di ring polinomial.

Konsep yang dibutuhkan untuk mengkontruksi ring faktor atas ideal yang dibangun oleh elemen di ring polinomial, seperti $R = \mathbb{Z}[x]/(x^N - 1)$. Diberikan ring $\mathbb{Z}$, maka dapat dibentuk suatu ring polinomial $\mathbb{Z}[x]$. Misal $g(x)$ merupakan polinomial irredusibel berderajat N di $\mathbb{Z}$, maka ring faktor $\mathbb{Z}[x]/(x^N - 1)$ yang terbentuk ring komutatif dengan elemen satuan berderajat $n-1$. Pertama akan dibahas ring, yaitu definisi ring, sifat-sifat pada ring. Sifat-sifat dari ring tersebut nantinya sangat dibutuhkan ketika melakukan pembuktiian contoh maupun teorema. Kedua adalah ring polinomial, yaitu definisi ring polinomial dan sifat-sifat dari ring polinomial. Ketiga adalah ideal, yaitu definisi ideal dan ideal yang dibangun oleh elemen. Konsep ring polinomial dan ideal yang nantinya digunakan untuk mengkontruksi ring faktor sedemikian hingga terbentuk R.

Konsep kriptografi diperlukan penerapan sistem kriptografi NTRU terutama siistem kriptografi asimetris yaitu penggunaan kunci yang berbeda pada proses enkripsi dan dekripsi. Alur penelitian dimulali dari mengkaji sistematika sistem kriptografi NTRU, kemudia struktur aljabar yang digunakan seperti definisi, teorema dan materi yang bersumber dari buku maupun catatan perkuliahan. Penelitian ini dikaji menjadi dua bagian yaitu struktur aljabar dan kriptografi dengan alur penelitian sebagai berikut:



Gambar 1.1 Alur Penelitian

1.8. Sistematika Penulisan

Pembahasan dalam penelitian ini terbagi menjadi lima bab, yaitu :

1. BAB I (Pendahuluan) : Bab ini membahas mengenai Latar Belakang, Rumusan Masalah, Batasan Masalah, Tujuan Penelitian, Tinjauan Pustaka, Metode Penelitian dan Sistematika Penulisan.

2. BAB II (Dasar Teori) : Bab ini membahas mengenai dasar - dasar teori aljabar abstrak yang mendasari algoritma NTRU.

3. BAB III (Sistem Kriptografi NTRU) : Bab ini membahas tentang kriptografi,

struktur algoritma NTRU beserta contoh.

4. BAB IV (Penutup) : Bab ini berisi kesimpulan penelitian dan saran penelitian terhadap perkembangan penelitian ini untuk kedepannya.

BAB IV

PENUTUP

Berdasaarkan pembahasan mengenai sistem kriptografi NTRU dapat diambil beberapa kesimpulan dan saran sebagai berikut:

4.1. Kesimpulan

Berdasarkan studi litelatur yang telah dilakukan mengenai sistem kriptografi NTRU. Sehingga didapat kesimpulan sebagai berikut:

1. Kontruksi R dapat dilakukan dengan konsep ring faktor oleh suatu ideal yang dibangun oleh elemen di ring polinomial $R[x]$. Diberikan ring $\mathbb{Z}$ sedemikian hingga dapat dibentuk ring polinomial $\mathbb{Z}[x]$ yang merupakan daerah integral. Diberikan $g(x)$ merupakan polinomial irredusibel berderajat N di $\mathbb{Z}[x]$, maka ideal $\langle g(x) \rangle$ merupakan ideal utama. Akibatnya terbentuk ring faktor $\mathbb{Z}[x]/(x^N - 1)$.

2. Sistem kriptografi NTRU merupakan sistem yang dibentuk atas ring faktor polinomial. Pada penelitian ini pihak yang ingin berkomunikasi adalah Alice (penerima pesan) dan Bob (pengirim pesan). Tahap pertama adalah pembentukan kunci publik yang dilakukan oleh Alice. Dipilih polinomial $F(x)$ dan $G(x)$ yang merupakan anggota R. Selanjutnya Alice membentuk $f(x) = 1 + pF(x)$ dan $g(x) = pG(x)$. Dihitung nilai f^{-1} di R modulo q. Kemudian Alice membentuk kunci publik dengan menghitung $h(x) = f^{-1}(x)g(x) \pmod q$, lalu mengirim $h(x)$ kepada Bob. Memasuki

tahap kedua yaitu Bob menerima $h(x)$ dari Alice, selanjutnya Bob melakukan enkripsi. Dengan memilih pesan yang akan dikirim ke Alice yaitu $m(x)$ anggota R. Bob juga memilik $r(x) \in R$. Enkripsi dilakukan dengan menghitung $e_K(y) = r \cdot h + m \pmod{q}$ yang kemudian dikirim kepada Alice sebagai chiperteks. Tahap ketiga dinamakan dengan dekripsi dimana Alice menerima chiperteks dari Bob, tugas Alice adalah mencari pesan sebenarnya atau plainteks yang dikirimkan oleh Bob dengan menghitung
$d^K y = (f \cdot e_K(y) \mod q) \mod p$.

4.2. Saran

Setelah selesainya penelitian ini tentang sistem kriptografi NTRU, maka terdapat peluang untuk melakukan penelitian lebih lanjut diantaranya:

1. Perbandingan NTRU dengan sistem kriptografi Sebelumnya.
2. Ketahanan NTRU terhadap suatu serangan.

DAFTAR PUSTAKA

Ayushi, 2010, *A Symmetric Key Cryptographic Algoritm*, International Journal of Computer Application.

Fadilatul, N. I., 2018, *Kajian Tentang Kriptosistem McEliece Dalam Menghadapi Tantangan Komputer Kuantum Di Era Revolusi Industri 4.0*, Prosiding Seminar Nasional MIPA 2018:216-226.

Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, 1998,*NTRU: A Ring Based Public Key Cryptosystem. In Algorithmic Number Theory (ANTS III)*, Lecture Notes in Computer Science 1423, Springer-eVrlag, Berlin:267-288.

J. Hoffstein, J. Silverman, 2000, *Optimizations for NTRU. Public-Key Cryptography and Computational Number Theory*, Warsaw:11-15.

Hoffstein, J., 2014, *An Introduction to Matematical Cryptography*, Springer Science, Inc., New York.

Jaulmes, E. dan Joux, A., 2000, *Chosen-Ciphertext Attack against NTRU*, Prosiding ke 20 Annual International Cryptology Conference on Advances in Cryptograph:20-35.

Malik, D. S., 1997, *Fundamental of Abstract Algebra*, Mc-Graw-Hill, Inc., New York.

Paterson, M. B. dkk, 2019, *Cryptography Theory and Practice*, Taylor and Francis Group, Inc., US.

Rosen, Kenneth, 2011, *Elementary Number Theory and Its Application*, Pearson Education, Inc., Boston.

Saputra, Herlambang, 2009, *Kajian Tentang Komputer Kuantum Sebagai Pengganti Komputer Konvensional Di Masa Depan*, Jurnal Generic 4:15-18.

Wahyuni, S. dkk, 2016, *Teori Ring dan Modul*, Gadjah Mada University Press, Yogyakarta.

...

CURRICULUM VITAE

A. Biodata Pribadi

Nama Lengkap	: Yulia Fatin Lestari
Jenis Kelamin	: Perempuan
Tempat, Tanggal Lahir	: Jakarta, 14 Juli 1998
Alamat Asal	: Jl. Taruna no.56 Rt.06/Rw.02, Sukapura, Cilincing, Jakarta Utara, DKI Jakarta, 14140
Email	: yulia.fatinlestari@gmail.com
No. HP	: 082328297028

B. Latar belakang Pendidikan

SD Negeri Sukapura 01 Pagi	(2004-2010)
SMP Negeri 121 Jakarta	(2010-2013)
SMA Negeri 52 Jakarta	(2013-2016)
UIN Sunan Kalijaga Yogyakarta	(2016-2021)