IMPLEMENTASI ALGORITMA *RIVEST SHAMIR ADLEMAN* ATAS RING DEDEKIND UNTUK MENGAMANKAN PESAN TEKS

SKRIPSI

OLEH:
ZAKIYYA DZUL LADUNNIYYAH
NIM. 19610048

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2023

IMPLEMENTASI ALGORITMA *RIVEST SHAMIR ADLEMAN* ATAS RING DEDEKIND UNTUK MENGAMANKAN PESAN TEKS

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
Zakiyya Dzul Ladunniyyah
NIM. 19610048

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG
2023

IMPLEMENTASI ALGORITMA *RIVEST SHAMIR ADLEMAN* ATAS RING DEDEKIND UNTUK MENGAMANKAN PESAN TEKS

SKRIPSI

Oleh
Zakiyya Dzul Ladunniyyah
NIM. 19610048

Telah Disetujui Untuk Diuji
Malang, 29 November 2023

Dosen Pembimbing I	Dosen Pembimbing II
Muhammad Khudzaifah, M.Si.	Erna Herawati, M.Pd.
NIDT. 19900511 202321 1 029	NIDT. 19760723 20180201 2 222

Mengetahui,
Ketua Program Studi Matematika

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

IMPLEMENTASI ALGORITMA *RIVEST SHAMIR ADLEMAN* ATAS RING DEDEKIND UNTUK MENGAMANKAN PESAN TEKS

SKRIPSI

Oleh
Zakiyya Dzul Ladunniyyah
NIM. 19610048

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

Tanggal 13 Desember 2023

Ketua Penguji	: Prof. Dr. H. Turmudi, M.Si., Ph.D.	.....
Anggota Penguji I	: Mohammad Nafie Jauhari, M.Si.	.....
Anggota Penguji II	: Muhammad Khudzaifah, M.Si.	.....
Anggota Penguji III	: Erna Herawati, M.Pd.	.....

Mengetahui,
Ketua Program Studi Matematika

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

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama	:	Zakiyya Dzul Ladunniyyah
NIM	:	19610048
Program Studi	:	Matematika
Fakultas	:	Sains dan Teknologi
Judul Skripsi	:	Implementasi Algoritma Rivest Shamir Adleman atas Ring Dedekind untuk Mengamankan Pesan Teks

menyatakan dengan sebenarnya bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya saya sendiri. Bukan merupakan pengambilan data, tulisan atau pikiran orang lain yang saya akui sebagai hasil tulisan atau pikiran saya sendiri, kecuali dengan mencantumkan sumber cuplikan pada daftar pustaka. Apabila di kemudian hari terbukti atau dapat dibuktikan skripsi ini hasil jiplakan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Malang, 13 Desember 2023
Yang membuat pernyataan,

Zakiyya Dzul Ladunniyyah
NIM. 19610048

MOTO

“Sesungguhnya Allah SWT berfirman: Aku menurut prasangka hamba-Ku, Aku mengingatnya saat ia mengingat-Ku. Jika ia mengingat-Ku dalam kesendirian, maka Aku akan mengingatnya dalam kesendirian-Ku. Jika ia mengingat-Ku dalam keramaian, maka Aku akan mengingatnya dalam keramaian yang lebih baik dari keramaiannya.”

(HR. Bukhari dan Muslim)

PERSEMBAHAN

Skripsi ini penulis persembahkan untuk:
Orang tua penulis Bapak Ahmad Sumari dan Ibu Suharti yang senantiasa memberikan kasih sayang, dukungan, serta doa restu demi kebaikan dan keberhasilan penulis. Adik penulis Shofiyya Quthbil Ma'rifah dan Balqis Tajalliyal Haq, beserta keluarga besar yang telah memberikan semangat dan dukungan kepada penulis.

KATA PENGANTAR

Puji syukur kehadirat Allah SWT atas segala limpahan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Implementasi Algoritma *Rivest Shamir Adleman* atas Ring Dedekind untuk Mengamankan Pesan Teks" dengan baik. Sholawat serta salam semoga senantiasa tercurahkan kepada Nabi Muhammad SAW yang telah menuntun umat manusia dari zaman jahiliyah menuju zaman yang penuh dengan ilmu pengetahuan.

Selanjutnya penulis ucapkan terima kasih kepada seluruh pihak yang telah memberikan arahan serta bimbingan dalam penyusunan skripsi ini. Ucapan terima kasih penulis sampaikan, khususnya kepada:

1. Prof. Dr. H. M. Zainuddin, M.A., selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim Malang.
2. Prof. Dr. Hj. Sri Harini, M.Si., selaku dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
3. Dr. Elly Susanti, M.Sc., selaku ketua Program Studi Matematika Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. Muhammad Khudzaifah, M.Si., selaku dosen pembimbing I yang telah memberi bimbingan, arahan, ilmu, serta saran yang membangun kepada penulis.
5. Erna Herawati, M.Pd., selaku dosen pembimbing II yang telah memberikan ilmu, kritik, saran serta motivasi kepada penulis.
6. Prof. Dr. H. Turmudi, M.Si., Ph.D., selaku Ketua Penguji dalam ujian skripsi yang telah memberikan kritik dan saran yang bermanfaat bagi penulis.
7. Muhammad Nafie Jauhari, M.Si., selaku Anggota Penguji I dalam ujian skripsi yang telah memberikan kritik dan saran yang bermanfaat bagi penulis.
8. Angga Dwi Mulyanto, M.Si., selaku dosen wali yang telah memberikan motivasi dan nasihat kepada penulis.

9. Seluruh dosen Program Studi Matematika Universitas Islam Negeri Maulana Malik Ibrahim Malang yang telah memberikan banyak ilmu, nasihat serta motivasi selama perkuliahan kepada penulis.
10. Kedua orang tua, Adik, serta seluruh keluarga yang senantiasa memberikan do'a, dukungan, semangat, serta nasihat demi kebaikan dan keberhasilan penulis.
11. Seluruh teman-teman di Program Studi Matematika angkatan 2019 yang senantiasa memberi do'a, semangat, serta dukungan selama masa perkuliahan kepada penulis.
12. Semua pihak yang secara langsung maupun tidak langsung telah ikut memberikan bantuan dan dukungan dalam menyelesaikan skripsi ini.

Penulis berharap agar skripsi ini dapat menambah wawasan keilmuan dan memberikan manfaat baik untuk penulis maupun seluruh pihak yang membacanya.

Malang, 13 Desember 2023

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR SIMBOL

$\mathbb{Z}$	=	Bilangan bulat
$\mathbb{Z}^+$	=	Bilangan bulat positif
$\mathbb{Q}$	=	Bilangan rasional
$b \mid a$	=	b habis membagi a
$b \nmid a$	=	b tidak habis membagi a
$(R, +, \cdot)$	=	Ring R dengan operasi penjumlahan dan perkalian
I	=	Ideal dari suatu ring
$\langle X \rangle$	=	Ideal yang dibangun oleh X
P	=	Ideal prima
M	=	Ideal maksimal
R/I	=	Ring faktor atau *quotient ring*
$\varphi(n)$	=	Fungsi Euler
D	=	Ring Dedekind
$\lvert R/I \rvert$	=	Kardinalitas dari ring faktor

DAFTAR LAMPIRAN

ABSTRAK

Ladunniyyah, Zakiyya Dzul, 2023. **Implementasi Algoritma Rivest Shamir Adleman atas Ring Dedekind untuk Mengamankan Pesan Teks.** Skripsi. Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Muhammad Khudzaifah, M.Si. (II) Erna Herawati, M.Pd.

Kata Kunci: Kriptografi, Algoritma RSA, Ring Dedekind.

Penelitian ini membahas mengenai implementasi algoritma RSA atas ring Dedekind untuk mengamankan pesan teks. Implementasi ini dilakukan dengan memodifikasi proses pembentukan kunci, enkripsi, dan dekripsi dari algoritma kriptografi RSA agar sesuai dengan ring Dedekind yang digunakan. Pada algoritma ini ring Dedekind digunakan dalam proses pembentukan kunci, di mana pasangan bilangan prima pada algoritma RSA diganti dengan ideal-ideal maksimal pada ring Dedekind. Selain itu, fungsi Euler yang digunakan adalah fungsi Euler untuk ideal pada ring Dedekind yang berupa hasil kali dari kardinalitas grup unit. Selanjutnya, proses enkripsi dan dekripsi dilakukan sesuai dengan persamaan enkripsi dan dekripsi algoritma RSA. Tahapan penelitian yang dilakukan yaitu melakukan pembentukan kunci pada algoritma RSA atas ring Dedekind, selanjutnya mengontruksi algoritma enkripsi dan dekripsi untuk mengamankan pesan dengan RSA atas ring Dedekind. Kesimpulan dari penelitian ini adalah implementasi algoritma RSA atas ring Dedekind dapat menghasilkan kunci publik yang lebih luas di mana kunci publik yang digunakan merupakan sebarang bilangan positif anggota dari himpunan hasil kali ideal maksimal pada ring Dedekind.

ABSTRACT

Ladunniyyah, Zakiyya Dzul, 2023. **Implementation of Rivest Shamir Adleman's Algorithm over Dedekind Ring to Secure Text Messages.** Thesis. Mathematics Study Program, Faculty of Science and Technology, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Advisors: (I) Muhammad Khudzaifah, M.Si. (II) Erna Herawati, M.Pd.

Keywords: Cryptography, RSA algorithm, Ring Dedekind.

This study discusses the implementation of the RSA algorithm over the Dedekind ring to secure text messages. This implementation is done by modifying the key formation, encryption, and decryption processes of the RSA cryptographic algorithm to match the Dedekind ring used. In this algorithm, the Dedekind ring is used in the key formation process, where the prime number pairs in the RSA algorithm are replaced with maximum ideals in the Dedekind ring. In addition, the Euler function used is the Euler function for the ideal on the Dedekind ring which is the product of the cardinality of the unit group. Next, the encryption and decryption processes are carried out according to the encryption and decryption equation of the RSA algorithm. The research stage carried out is to form a key on the RSA algorithm over the Dedekind ring, then construct an encryption and decryption algorithm to secure messages with RSA over the Dedekind ring. The conclusion of this study is that the implementation of the RSA algorithm over the Dedekind ring can produce a wider public key where the public key used is any positive member number of the set of maximal ideal products on the Dedekind ring.

مستخلص البحث

لدنية، زكية ذول، ٢٠٢٣. **تنفيذ خوارزمية رافيست وشامير وأدلمن عبر حلقة دِيدِ كاند لتأمين الرسائل النصية**. البحث الجامعي. قسم الرياضيات، كلية العلوم والتكنولوجيا بجامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج. المشرف الأول: محمد خذيفة، الماجستير. المشرف الثاني: إرنا هيراواتي، الماجستيرة.

الكلمات الرئيسية: تشفير، خوارزمية آر إس إيه، حلقة ديد كاند.

ناقش هذا البحث تنفيذ خوارزمية آر إس إيه عبر حلقة ديد كاند لتأمين الرسائل النصية. تم هذا التنفيذ عن طريق تعديل عمليات تكوين المفاتيح والتشفير وفك التشفير لخوارزمية تشفير آر إس إيه لتتناسب مع حلقة ديد كاند المستخدمة. في هذه الخوارزمية، يتم استخدام حلقة ديد كاند في عملية تشكيل المفتاح، حيث يتم استبدال أزواج الأرقام الأولية في خوارزمية آر إس إيه بأقصى قدر من المثل العليا في حلقة ديد كاند. بالإضافة إلى ذلك، فإن وظيفة أويلر المستخدمة هي وظيفة أويلر للمثالية على حلقة ديد كاند التي هي نتاج العلاقة الأساسية لمجموعة الوحدات. بعد ذلك، يتم تنفيذ عمليات التشفير وفك التشفير وفقا لمعادلة التشفير وفك التشفير لخوارزمية آر إس إيه. تتمثل مرحلة البحث التي يتم إجراؤها في تشكيل مفتاح على خوارزمية آر إس إيه عبر حلقة ديد كاند، ثم إنشاء خوارزمية تشفير وفك تشفير لتأمين الرسائل باستخدام آر إس إيه عبر حلقة ديد كاند. الاستنتاج من هذا البحث هو أن تنفيذ خوارزمية آر إس إيه على حلقة ديد كاند يمكن أن ينتج مفتاحا عاما أوسع حيث يكون المفتاح العام المستخدم هو أي عضو رقم موجب في مجموعة المنتجات المثالية القصوى على حلقة ديد كاند.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi di bidang informasi dan komunikasi dapat memberikan dampak positif di antaranya yaitu memberi kemudahan dalam proses pertukaran informasi. Informasi dapat berupa pesan atau data yang adakalanya bersifat rahasia karena berisi hal-hal penting yang perlu dijaga keamanannya sehingga tidak dapat diakses, diketahui, ataupun disalahgunakan oleh pihak yang tidak bertanggung jawab. Kemajuan teknologi juga dapat memberikan dampak negatif, seperti mempermudah aktivitas kejahatan yang dapat mengganggu privasi seseorang. Beberapa hal yang telah terjadi di Indonesia di antaranya yaitu penyadapan atau pencurian data-data pribadi untuk disalahgunakan sehingga dapat merugikan korban. Hal ini menunjukkan bahwa masalah keamanan dan kerahasiaan data atau pesan merupakan hal yang penting sehingga diperlukan upaya untuk menjaga keamaan dan kerahasiaan dari suatu pesan atau data.

Kriptografi merupakan metode yang dapat digunakan untuk menjaga kerahasiaan dan keamanan suatu pesan atau data sehingga pesan hanya dapat dipahami oleh pihak yang dituju. Kriptografi merupakan ilmu sekaligus seni untuk menjaga keamanan pesan dengan menyandikan pesan tersebut menjadi pesan acak yang tidak bermakna (Munir, 2016). Tujuan dari kriptografi bukan untuk menyembunyikan pesan, melainkan menyembunyikan makna dari suatu pesan. Pesan asli (plainteks) akan diubah menjadi pesan yang telah disandikan (cipherteks) dengan kunci tertentu sehingga pesan hanya dapat diketahui oleh pihak yang dituju.

Proses ini disebut sebagai proses enkripsi. Sebaliknya, proses untuk mengembalikan cipherteks menjadi plainteks disebut dekripsi.

Allah SWT berfirman dalam Al-Qur'an Surah Al-Anfal ayat 27 sebagai berikut (Lajnah Pentashihan Mushaf Al-Qur'an, 2018):

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا تَخُوْنُوا اللّٰهَ وَالرَّسُوْلَ وَتَخُوْنُوْٓا اَمٰنٰتِكُمْ وَاَنْتُمْ تَعْلَمُوْنَ ﴿٢٧﴾

Artinya: *"Wahai orang-orang yang beriman, janganlah kamu mengkhianati Allah SWT dan Rasul SAW serta janganlah kamu mengkhianati amanat yang dipercayakan kepadamu, sedangkan kamu mengetahui".*

Ayat ini berisi perintah untuk tidak mengkhianati Allah SWT dan Rasul-Nya dengan senantiasa menjalankan perintah-Nya serta menjauhi segala larangan-Nya yang telah ditentukan dalam Al-Qur'an dan Hadits. Selain itu, Allah memerintahkan umat-Nya untuk tidak mengkhianati amanat yang telah dipercayakan baik berupa benda, perbuatan, perkataan, maupun kepercayaan. Amanat erat kaitannya dengan kepercayaan, karena ketika amanat tidak lagi terpelihara maka hilanglah kepercayaan yang berakibat tidak adanya ketenangan hidup dalam bermasyarakat (Kemenag, 2019). Adapun mengembalikan titipan kepada pemiliknya, tidak menipu, serta memelihara rahasia merupakan salah satu bentuk sifat amanah. Hal ini menunjukkan bahwa menjaga kerahasiaan pesan sehingga pesan diterima oleh pihak yang berhak menerima merupakan salah satu bentuk melaksanakan amanah. Amanah berupa pesan atau data perlu dijaga agar pesan atau data dapat sampai kepada pihak yang menerima tanpa adanya perubahan yang dilakukan oleh pihak ketiga. Hal ini sesuai dengan konsep kriptografi di mana pesan akan disandikan sehinga hanya dapat dipahami oleh pihak yang berhak menerima tanpa adanya perubahan.

Algoritma kriptografi merupakan urutan untuk menyelesaikan masalah yang disusun secara sistematis dalam proses menyandikan pesan. Pada dasarnya

proses penyandian pesan didasari oleh tiga fungsi yaitu kunci, enkripsi, dan dekripsi. Enkripsi merupakan proses mengubah pesan menjadi pesan acak, sedangkan dekripsi merupakan proses mengembalikan pesan acak menjadi pesan awal. Proses enkripsi dan dekripsi ini dilakukan dengan menggunakan kunci yang telah disepakati oleh pihak yang berkonumikasi. Berdasarkan jenis kunci yang digunakan, algoritma kriptografi dibagi menjadi algoritma simetri dan algoritma asimetri. Algoritma simetri menggunakan kunci yang sama untuk proses enkripsi dan dekripsinya. Sedangkan pada algoritma asimetri kunci yang digunakan berbeda, yaitu kunci publik untuk proses enkripsi dan kunci privat untuk proses dekripsi (Munir, 2006). Salah satu algoritma kriptografi dengan kunci publik yaitu *Rivest Shamir Adleman* (RSA) yang ditemukan oleh Ronald Rivest, Adi Shamir, dan Len Adleman pada tahun 1976. Kunci publik RSA merupakan hasil perkalian dua bilangan prima besar yang kemudian digunakan pada proses enkripsi (Munir, 2016).

Algoritma RSA memiliki pengaruh yang besar dalam perkembangan teori bilangan dengan menunjukkan bahwa teori bilangan juga memiliki kegunaan yang penting. Secara umum, algoritma RSA menunjukkan bahwa cukup mudah untuk mengalikan dua bilangan prima besar, namun sulit untuk memfaktorkan bilangan menjadi faktor primanya dengan efisien (Hodge et al., 2013). Oleh sebab itu, topik mengenai faktorisasi dan menemukan bilangan prima menjadi populer dan terus mengalami kemajuan. Bahkan hingga tahun 2013, batas kemampuan teknologi dalam faktorisasi bilangan telah mencapai 230 digit bilangan (Kraft & Washington, 2016). Hal ini menunjukkan bahwa terdapat kemungkinan segera ditemukannya algoritma yang efisien untuk faktorisasi sehingga beberapa algoritma kriptografi,

seperti RSA, terancam dapat dipecahkan. Sehingga telah dilakukan beberapa penelitian mengenai modifikasi algoritma RSA dengan tujuan meningkatkan keamanan dari algoritma tersebut.

Ring Dedekind merupakan salah satu ring penting dalam aljabar yang memiliki banyak karakteristik dan kegunaan, salah satunya pada ilmu kriptografi. Ring Dedekind pertama kali diperkenalkan pada tahun 1879 oleh Julius Wilhelm Richard Dedekind. Dalam aljabar abstrak, ring Dedekind adalah ring dengan setiap ideal tak nolnya dapat difaktorkan menjadi hasil kali dari ideal-ideal prima (Persulessy & Dahoklory, 2015). Suatu ring disebut Dedekind jika dan hanya jika tertutup secara integral, berupa ring *noetherian*, dan setiap ideal tak nolnya adalah ideal maksimal. Beberapa contoh ring Dedekind di antaranya adalah ring $\mathbb{Z}$, ring $\mathbb{Z}[i]$, dan ring polinomial (Jankowska & Matysiak, 2022).

Penelitian mengenai implementasi algoritma kriptografi atas ring Dedekind sebelumnya beberapa kali telah dilakukan, yaitu dengan memodifikasi proses pembentukan kunci maupun proses enkripsi dan dekripsinya sesuai dengan ring Dedekind yang digunakan. El-Kassar, Ramzi Haraty, dan Yahia Awad (2005) melakukan penelitian mengenai modifikasi algoritma RSA pada ring Gaussian dan ring polinomial. Pada algoritma RSA untuk ring Gaussian, pasangan bilangan prima diganti dengan pasangan bilangan prima pada ring Gaussian sedangkan pada ring polinomial, dibutuhkan dua polinomial untuk proses pembentukan kuncinya. Penelitian ini menunjukkan bahwa algoritma yang telah dimodifikasi memiliki jangkauan yang lebih luas dan proses pembentukan kuncinya menjadi lebih rumit. Namun, setiap algoritma RSA yang dihasilkan hanya berlaku untuk salah satu jenis ring Dedekind. Selanjunya pada penelitian Jankowska dan Matysiak (2022),

peneliti membentuk algoritma kriptografi berdasarkan struktur dari ring Dedekind. Beberapa algoritma yang dihasilkan dalam penelitian ini yaitu kriptosistem dengan kunci berupa ideal fraksional, kriptosistem dengan alfabet berupa ideal fraksional, serta aplikasi polinomial pada kriptologi (Jankowska & Matysiak, 2022).

Berdasarkan penelitian yang telah dikemukakan sebelumnya, dalam penelitian ini akan dilakukan implementasi algoritma RSA atas ring Dedekind. Pada algoritma ini, ring Dedekind digunakan pada proses pembentukan kunci yaitu pasangan bilangan prima pada RSA akan diganti dengan ideal-ideal pada ring Dedekind. Selanjutnya fungsi Euler yang digunakan adalah fungsi Euler untuk ideal yang berupa hasil kali dari kardinalitas grup unit. Selanjutnya dilakukan proses enkripsi dan dekripsi untuk meyandikan pesan teks dengan algoritma RSA.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana proses pembentukan kunci pada algoritma RSA atas ring Dedekind?
2. Bagaimana proses enkripsi menggunakan algoritma RSA atas ring Dedekind untuk mengamankan pesan teks?
3. Bagaimana proses dekripsi menggunakan algoritma RSA atas ring Dedekind untuk mengamankan pesan teks?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, tujuan dari penelitian ini adalah sebagai berikut:

1. Untuk mengetahui proses pembentukan kunci pada algoritma RSA atas ring Dedekind.
2. Untuk mengetahui proses enkripsi menggunakan algoritma RSA atas ring Dedekind untuk mengamankan pesan.
3. Untuk mengetahui proses dekripsi menggunakan algoritma RSA atas ring Dedekind untuk mengamankan pesan.

1.4 Manfaat Penelitian

Hasil dari penelitian ini diharapkan dapat memberi manfaat sebagai berikut:

1. Bagi penulis

   Menambah wawasan penulis mengenai ring Dedekind dan kriptografi khususnya algoritma RSA serta mengetahui algoritma RSA atas ring Dedekind.
2. Bagi pembaca
   a. Dapat menambah wawasan mengenai ilmu kriptografi khususnya algoritma RSA atas ring Dedekind.
   b. Sebagai referensi untuk penelitian selanjutnya dalam mengimplementasikan algoritma RSA atas ring Dedekind.

1.5 Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Pada proses penyandian karakter yang digunakan berupa huruf, angka, dan simbol berdasarkan ASCII *printable character*.
2. Ring Dedekind yang digunakan pada simulasi algoritma RSA atas ring Dedekind adalah ring $\mathbb{Z}$.

1.6 Definisi Istilah

Beberapa istilah yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Enkripsi

   Enkripsi merupakan proses menyandikan pesan asli menjadi pesan acak yang tidak bermakna dengan kunci yang telah disepakati.

2. Dekripsi

   Dekripsi merupakan proses mengembalikan pesan acak menjadi pesan asli menggunakan kunci yang telah disepakati.

3. Algoritma Kriptografi

   Algoritma kriptografi adalah urutan untuk menyelesaikan masalah yang disusun secara sistematis dalam proses penyandian pesan atau data yang bertujuan untuk menjaga keamanan dan kerahasian pesan atau data.

4. Algoritma RSA

   Algoritma RSA adalah salah satu algoritma kriptografi kunci publik yang menggunakan kunci yang berbeda pada proses penyandian pesan, yaitu kunci publik untuk proses enkripsi dan kunci privat untuk proses dekripsi.

5. Ring

   Ring merupakan struktur aljabar yang terdiri dari himpunan tak kosong dan menggunakan dua operasi biner, yaitu operasi penjumlahan dan operasi perkalian.

BAB II
KAJIAN TEORI

2.1 Teori Pendukung

2.1.1 Teori Bilangan

2.1.1.1 Keterbagian

Definisi 2.1

Misalkan $a, b \in \mathbb{Z}$ dengan $b > 0$. b dikatakan membagi a, ditulis sebagai $b|a$, jika terdapat $q \in \mathbb{Z}$ sedemikian sehingga $a = bq$ dan b disebut sebagai pembagi a. Jika tidak terdapat $q \in \mathbb{Z}$, maka b tidak membagi a, ditulis sebagai $b \nmid a$ (Kraft & Washington, 2016).

Contoh 2.1

5 membagi 30, ditulis sebagai $5|30$, karena terdapat bilangan bulat $q = 6$ sedemikian sehingga $30 = 5 \cdot 6$. Sedangkan 5 tidak membagi 102, ditulis sebagai $5 \nmid 102$, karena tidak terdapat bilangan bulat q yang memenuhi $102 = 5 \cdot q$.

Teorema 2.1

Misalkan $a, b, c \in \mathbb{Z}$. Jika $a|b$ dan $b|c$ maka $a|c$ (Kraft & Washington, 2016).

Bukti:

Kerena $a|b$ maka terdapat $q \in \mathbb{Z}$ sedemikian sehingga $b = aq$, dan $b|c$ maka terdapat $p \in \mathbb{Z}$ sedemikian sehingga $c = bp$.

Kemudian untuk c diperoleh

$$c = bp = (aq)p = a(qp)$$

dengan $p, q \in \mathbb{Z}$. Dengan demikian $a|c$. ■

Teorema 2.2

Misalkan $a, b, d, x, y \in \mathbb{Z}$. Jika $d|a$ dan $d|b$ maka $d|ax + by$ (Kraft & Washington, 2016)

Bukti:

Karena $d|a$ maka $a = dp$ dan $d|b$ maka $b = dq$, dengan $p, q \in \mathbb{Z}$.

Selanjutnya untuk $ax + by$,

$$ax + by = (dp)x + (dq)y = d(px) + d(qy) = d(px + qy)$$

Dengan demikian $d|ax + by$. ■

Teorema 2.3

Misalkan $a, b, d \in \mathbb{Z}$. Jika $d|a$ dan $d|b$ maka $d|a + b$ dan $d|a - b$ (Kraft & Washington, 2016)

Bukti:

Karena $d|a$ maka $a = dp$ dan $d|b$ maka $b = dq$, dengan $p, q \in \mathbb{Z}$.

Akan ditunjukkan bahwa $d|a + b$,

$$a + b = dp + dq = d(p + q)$$

Dengan demikian $d|a + b$. Selanjutnya akan ditunjukkan bahwa $d|a - b$,

$$a - b = dp - dq = d(p - q)$$

Dengan demikian $d|a - b$. ■

2.1.1.2 Aritmetika Modulo

Aritmetika modulo merupakan metode aritmetika yang digunakan dalam menyelesaikan masalah-masalah yang berkaitan dengan bilangan bulat. Aritmetika modulo memiliki peran penting dalam komputasi bilangan bulat, khususnya pada proses enkripsi dan dekripsi dalam kriptografi. Operator yang

digunakan dalam aritmetika modulo adalah mod, yang memberikan sisa pembagian (Ginting, 2010).

Definisi 2.2

Misalkan $a \in \mathbb{Z}$ dan $m \in \mathbb{Z}^+$. Operasi $a \bmod m$ memberikan sisa r jika a dibagi dengan m. Hal ini dinotasikan dengan $a \bmod m = r$ sedemikian sehingga $a = mq + r$, dengan q adalah hasil bagi, r adalah sisa bagi, dan $0 \leq r < m$. Bilangan m disebut dengan modulo atau modulus dan hasil aritmetika modulo terletak dalam himpunan $\{0, 1, \ldots, m-1\}$ (Linuhung, 2018).

Contoh 2.2

$127 \bmod 85 = 42$, karena $a = 127$ dibagi dengan $m = 85$ diperoleh hasil bagi $q = 1$ dan sisa bagi $r = 42$, atau dapat ditulis sebagai $127 = 1 \cdot 85 + 42$.

2.1.1.3 Kongruensi

Ide mengenai kongruensi banyak digunakan untuk mendeskripsikan fenomena siklik pada bilangan bulat (Hodge et al., 2013). Konsep mengenai kongruensi juga dapat digunakan ketika mengelompokkan bilangan bulat sebagai bilangan genap atau ganjil. Secara umum, dua bilangan dikatakan kongruen terhadap n jika dua bilangan tersebut memiliki sisa bagi yang sama ketika dibagi dengan n (Kraft & Washington, 2016).

Definisi 2.3

Misalkan $n \in \mathbb{N}$ dan $a, b \in \mathbb{Z}$. a kongruen b modulo n, dinotasikan sebagai $a \equiv b \pmod{n}$, jika n membagi $a - b$. Jika n tidak membagi $a - b$ maka a dikatakan tidak kongruen dengan b modulo n, ditulis sebagai $a \not\equiv b \pmod{n}$. (Hodge et al., 2013).

Contoh 2.3

22 kongruen dengan 4 modulo 9, ditulis sebagai $22 \equiv 4 \pmod 9$, karena 9 habis membagi $(22-4)$, tetapi 22 tidak kongruen dengan 11 modulo 9 karena 9 tidak habis membagi $(22-11)$.

Teorema 2.4

Misalkan $a, b \in \mathbb{Z}$ maka $a \equiv b \pmod n$ jika dan hanya jika terdapat $k \in \mathbb{Z}$ sedemikian sehingga $a = b + kn$ (Kraft & Washington, 2016).

Bukti:

$\Rightarrow$ Jika $a \equiv b \pmod n$ maka $n|(a-b)$. Dengan demikian terdapat $k \in \mathbb{Z}$ sedemikian sehingga

$$(a-b) = kn$$

$$\Leftrightarrow \quad a = b + kn$$

$\Leftarrow$ Jika terdapat $k \in \mathbb{Z}$ sedemikian sehingga $a = b + kn$ maka

$$a = b + kn$$

$$\Leftrightarrow \quad a - b = kn$$

$$\Leftrightarrow \quad n \mid (a-b)$$

Dengan demikian $a \equiv b \pmod n$. ■

Teorema 2.5

Misalkan $a, b, c, n \in \mathbb{Z}$ dengan $n > 0$, kongruensi modulo n memenuhi beberapa sifat berikut (Hodge et al., 2013):

1. Sifat reflektif, yaitu $a \equiv a \pmod n$.
2. Sifat simetris, yaitu jika $a \equiv b \pmod n$ maka $b \equiv a \pmod n$.
3. Sifat transitif, yaitu jika $a \equiv b \pmod n$ dan $b \equiv c \pmod n$ maka $a \equiv c \pmod n$.

Bukti:

1. Karena terdapat $k = 0$ sedemikian sehingga $a = a + 0 \cdot n$ maka berdasarkan Teorema 2.4, diperoleh

$$\begin{aligned} & a = b + 0n \\ \Leftrightarrow \quad & a - b = 0 \\ \Leftrightarrow \quad & a = b \end{aligned}$$

   Dengan demikian $a \equiv a \pmod{n}$

2. Jika $a \equiv b \pmod{n}$ maka $a = b + kn$ dengan $k \in \mathbb{Z}$. Dengan demikian,

$$\begin{aligned} & (-b) = (-a) + kn \\ \Leftrightarrow \quad & b = a + (-kn) \\ \Leftrightarrow \quad & b = a + (-k)n \end{aligned}$$

   Berdasarkan Teorema 2.4, maka $b \equiv a \pmod{n}$

3. Jika $a \equiv b \pmod{n}$ maka terdapat k_1 sedemikian sehingga $a - b = k_1 n$, dan jika $b \equiv c \pmod{n}$ maka terdapat k_2 sehingga $b - c = k_2 n$, dengan $k_1, k_2 \in \mathbb{Z}$. Dengan demikian,

$$\begin{aligned} a - c &= (a - b) + (b - c) \\ &= (k_1 n) + (k_2 n) \\ &= (k_1 + k_2)n \end{aligned}$$

   sehingga $a \equiv c \pmod{n}$. ■

2.1.1.4 Fungsi Euler

Seorang matematikawan Swiss, Leonhard Euler, mempelajari serta melakukan pembuktian terhadap beberapa hasil penelitian Fermat mengenai teori bilangan. Euler memberikan perluasan terhadap teorema kecil Fermat

yang pada akhirnya disebut dengan Teorema Euler (Kraft & Washington, 2016).

Definisi 2.4

Fungsi ϕ −Euler merupakan fungsi yang memulihkan jumlah bilangan bulat j dengan $0 < j < n$ sedemikian sehingga $\gcd(j, n) = 1$ di mana $n \in \mathbb{Z}^+$. (Kraft & Washington, 2016).

Contoh 2.4

$\phi(7) = 6$ karena terdapat $j_1 = 1,\ j_2 = 2,\ j_3 = 3,\ j_4 = 4,\ j_5 = 5$ dan $j_6 = 6$ dengan $\gcd(j_i, 7) = 1$. Secara umum, untuk sebarang p bilangan prima, maka $\phi(p) = p - 1$ (Kraft & Washington, 2016).

Selanjutnya, akan ditunjukkan hasil utama dari penelitian Euler yang berupa Teorema Euler.

Teorema 2.6 Teorema Euler

Misalkan n adalah bilangan bulat positif dan b adalah bilangan bulat dengan $\gcd(b, n) = 1$. Maka

$$b^{\phi(n)} \equiv 1 (mod\ n)$$

2.1.2 Ring

2.1.2.1 Definisi Ring

Definisi 2.5

Misalkan R adalah himpunan tak kosong dengan dua operasi biner yaitu penjumlahan dan perkalian yang dinotasikan sebagai $+$ dan $\cdot$. Himpunan R adalah ring jika memenuhi:

1. Himpunan R tertutup atas operasi penjumlahan dan perkalian, yaitu untuk setiap $x, y \in R$ berlaku

$$x + y \in R \text{ dan } x \cdot y \in R$$

2. Operasi penjumlahan dan perkalian di R bersifat asosiatif, yaitu untuk setiap $x, y, z \in R$ berlaku

$$(x + y) + z = x + (y + z) \text{ dan } (x \cdot y) \cdot z = x \cdot (y \cdot z)$$

3. Operasi penjumlahan di R bersifat komutatif, yaitu untuk setiap $x, y \in R$ berlaku

$$x + y = y + x$$

4. Himpunan R memiliki unsur identitas yang disebut elemen nol, sehingga untuk setiap $x \in R$ terdapat $0_R \in R$ sedemikian sehingga

$$x + 0_R = 0_R + x = x$$

5. Setiap elemen di di R memiliki elemen invers di R, yang berarti untuk setiap $x \in R$ terdapat $-x \in R$ sedemikian sehingga

$$x + (-x) = (-x) + x = 0_R$$

6. Operasi perkalian dan penjumlahan di di R bersifat distributif, sehingga untuk setiap $x, y, z \in R$ berlaku

$$(x + y) \cdot z = x \cdot z + y \cdot z \text{ dan } x \cdot (y + z) = x \cdot y + x \cdot z$$

yang disebut distributif kanan dan distributif kiri (Hodge et al., 2013).

Contoh 2.5

Himpunan $\mathbb{Z}$ merupakan ring atas operasi penjumlahan dan perkalian, karena memenuhi sifat-sifat pada Definisi 2.5 berikut:

1. Untuk setiap $p, q \in \mathbb{Z}$ berlaku $p + q \in \mathbb{Z}$ dan $p \cdot q \in \mathbb{Z}$, sehingga himpunan $\mathbb{Z}$ tertutup atas operasi penjumlahan dan perkalian.

2. Untuk setiap $p, q, r \in \mathbb{Z}$ berlaku $(p + q) + r = p + (q + r)$ dan $(p \cdot q) \cdot r = p \cdot (q \cdot r)$. Sehingga operasi penjumlahan dan perkalian pada himpunan $\mathbb{Z}$ bersifat asosiatif.
3. Untuk setiap $p, q \in \mathbb{Z}$ berlaku $p + q = q + p$ dan$p \cdot q = q \cdot p$, sehingga operasi penjumlahan dan perkalian pada himpunan $\mathbb{Z}$ bersifat komutatif.
4. Himpunan $\mathbb{Z}$ memiliki unsur identitas atas operasi penjumlahan, yaitu $0 \in \mathbb{Z}$, sedemikian sehingga untuk setiap $p \in \mathbb{Z}$ berlaku $p + 0 = 0 + p = p$.
5. Himpunan $\mathbb{Z}$ memiliki elemen invers yaitu untuk setiap $p \in \mathbb{Z}$ terdapat $-p \in \mathbb{Z}$ sehingga berlaku $p + (-p) = (-p) + p = 0$.
6. Untuk setiap $p,\ q,\ r \in \mathbb{Z}$ berlaku $(p + q) \cdot r = (p \cdot r) + (q \cdot r)$ dan $p \cdot (q + r) = (p \cdot q) + (p \cdot r)$. Sehingga berlaku sifat distributif terhadap operasi penjumlahan dan perkalian.

2.1.2.2 Elemen Satuan

Definisi 2.6

Diberikan suatu ring $(R, +, \cdot)$. Jika terdapat $e \in R$ untuk setiap $x \in R$ sedemikian sehingga $ex = x$ maka e disebut elemen satuan kiri. Jika terdapat $e \in R$ untuk setiap $x \in R$ sedemikian sehingga $xe = x$ maka e disebut elemen satuan kanan. Selanjutnya, $e \in R$ disebut elemen satuan jika untuk setiap $x \in R$ berlaku $ex = xe = x$ (Hungerford, 2000).

Contoh 2.6

Pada ring $(\mathbb{Z}, +, \cdot)$ terdapat elemen e yaitu $e = 1 \in \mathbb{Z}$ sedemikian sehingga untuk setiap $p \in R$ berlaku $p1 = 1p = p$. Dengan demikian e disebut sebagai elemen satuan pada ring $\mathbb{Z}$.

2.1.2.3 Ring Komutatif dengan Elemen Satuan

Definisi 2.7

Diberikan suatu ring $(R, +, \cdot)$. Ring R disebut ring komutatif jika R komutatif terhadap perkalian, yang berarti untuk setiap $x, y \in R$ berlaku

$$xy = yx$$

dan disebut ring dengan elemen satuan jika R memiliki unsur identitas terhadap operasi perkalian, yang disebut elemen satuan. Hal ini berarti terdapat $e \in R$ sedemikian sehingga untuk setiap $x \in R$ berlaku

$$xe = ex = x$$

Selanjutnya, jika R merupakan ring komutatif dan mempunyai elemen satuan terhadap perkalian, maka ring R disebut ring komutatif dengan elemen satuan (Wahyuni et al., 2017).

Contoh 2.7

Pada ring $(\mathbb{Z}, +, \cdot)$, untuk setiap $p, q \in \mathbb{Z}$ berlaku sifat komutatif yaitu $pq = qp$, sehingga ring $\mathbb{Z}$ merupakan ring komutatif. Selanjutnya berdasarkan Contoh 2.6, ring $\mathbb{Z}$ terdapat elemen satuan yaitu $e = 1$. Dengan demikian $\mathbb{Z}$ merupakan ring komutatif dengan elemen satuan.

2.1.2.4 Elemen Unit

Definisi 2.8

Diberikan suatu ring R dengan elemen satuan e. Suatu elemen $u \in R$ disebut sebagai unit di R jika u memiliki invers terhadap operasi perkalian, yaitu terdapat $u^{-1} \in R$ sedemikian sehingga $u^{-1}u = uu^{-1} = e$ (Wahyuni et al., 2017).

Contoh 2.8

Pada ring $(\mathbb{Z}, +, \cdot)$ hanya terdapat dua elemen yang memiliki invers terhadap perkalian yaitu 1 dan (-1). Untuk $1 \in \mathbb{Z}$ terdapat $u^{-1} = 1 \in \mathbb{Z}$ sedemikian sehingga $1 \cdot 1 = 1$. Selanjutnya, untuk $(-1) \in \mathbb{Z}$ terdapat $u^{-1} = (-1) \in \mathbb{Z}$ sedemikian sehingga $(-1) \cdot (-1) = 1$. Dengan demikian, unit pada ring $(\mathbb{Z}, +, \cdot)$ adalah 1 dan (-1).

2.1.3 Ideal

2.1.3.1 Definisi Ideal

Definisi 2.9

Misalkan S adalah himpunan bagian tak kosong dari ring $(R, +, \cdot)$. Himpunan S disebut subring dari R jika S adalah ring dengan operasi penjumlahan dan perkalian yang sama dengan R. Selanjutnya, misalkan R adalah ring dan himpunan tak kosong $I \subset R$. Himpunan I disebut ideal kiri jika dan hanya jika memenuhi:

1. Untuk setiap $x, y \in I$ maka $x - y \in I$
2. Untuk setiap $x \in I$ dan $a \in R$ maka $ax \in I$

Subring I disebut ideal kanan jika dan hanya jika memenuhi:

1. Untuk setiap $x, y \in I$ maka $x - y \in I$
2. Untuk setiap $x \in I$ dan $a \in R$ maka $xa \in I$

Jika untuk setiap $x \in I$ dan $a \in R$ berlaku $xa = ax \in I$, maka I disebut sebagai *two sided ideal* (ideal dua sisi) (Wahyuni et al., 2017).

Berdasarkan definisi ideal dan definisi subring diatas, dapat diketahui bahwa ideal I merupakan subring dari R. Dengan demikian, dapat diambil kesimpulan bahwa setiap ideal I dari ring R adalah subring dari R.

Namun, untuk sebaliknya belum tentu berlaku, yaitu setiap subring I dari ring R belum tentu ideal dari R. Setiap ring R mempunyai dua ideal tak sejati, yaitu R dan $E = \{0_R\}$, yang disebut sebagai ideal trivial. Ideal I selain R dan E disebut sebagi ideal sejati.

Contoh 2.9

Diberikan ring $(\mathbb{Z}, +, \cdot)$. Misalkan diambil himpunan $2\mathbb{Z} \subset \mathbb{Z}$. Himpunan $2\mathbb{Z}$ merupakan ideal sejati pada ring $\mathbb{Z}$, sedangkan ideal trivial pada ring $\mathbb{Z}$ adalah $\mathbb{Z}$ itu sendiri dan $\{0\}$. Secara umum, untuk setiap $k \in \mathbb{Z}^{\geq 0}, k\mathbb{Z} = \{kn | n \in \mathbb{Z}\}$ merupakan ideal di ring $\mathbb{Z}$.

Misalkan X adalah himpunan bagian dari ring R dengan $X \neq \emptyset$. Ideal $\langle X \rangle$ disebut sebagai ideal yang dibangun oleh X. Jika $\langle X \rangle = R$ maka R disebut sebagai ring yang dibangun oleh X. Dengan demikian elemen dari himpunan X merupakan pembangun dari ideal $\langle X \rangle$. Jika $X = \{x_1, x_2, \dots, x_n\}$ maka ideal $\langle X \rangle$ dinotasikan sebagai $\langle x_1, x_2, \dots, x_n \rangle$ dan disebut *finitely generated* atau dibangun secara berhingga.

2.1.3.2 Ideal Prima

Definisi 2.10

Misalkan R adalah ring dan P adalah ideal dari ring R. Ideal P disebut ideal prima jika untuk setiap dua ideal A dan B di R dengan $AB \subseteq P$ berakibat $A \subseteq P$ atau $B \subseteq P$ (Wahyuni et al., 2017).

Contoh 2.10

Pada ring $(\mathbb{Z}, +, \cdot)$, misalkan diambil ideal $P = \langle 5 \rangle$. Diambil sebarang ideal A dan B di $\mathbb{Z}$ sedemikian sehingga $AB \subseteq P$. Karena A dan B merupakan ideal di $\mathbb{Z}$, maka terdapat $a, b \in \mathbb{Z}$ sedemikian sehingga $A = \langle a \rangle$ dan $B = \langle b \rangle$. Dengan

demikian, diperoleh $ab\mathbb{Z} = \langle a\rangle\langle b\rangle \subseteq P$ dengan ab merupakan bilangan kelipatan 5 sehingga diperoleh $a \in P$ atau $b \in P$. Hal ini berakibat $\langle a\rangle \subseteq P$ atau $\langle b\rangle \subseteq P$.

2.1.3.3 Ideal Maksimal

Definisi 2.11

Misalkan R adalah ring dan M adalah ideal dari ring R dengan $M \neq R$. Ideal M dikatakan maksimal jika dan hanya jika tidak terdapat ideal N di R sedemikian sehingga $M \subset N \subset R$ (Wahyuni et al., 2017).

Contoh 2.11

Misalkan $(\mathbb{Z}, +, \cdot)$ adalah ring komutatif dengan elemen satuan. $M = \langle 5\rangle$ adalah ideal maksimal di $\mathbb{Z}$ karena M tidak termuat dalam ideal lain di ring $\mathbb{Z}$ kecuali M dan $\mathbb{Z}$ itu sendiri.

2.1.3.4 Ring Faktor

Definisi 2.12

Misalkan R adalah ring dan I adalah ideal dari R. R/I adalah himpunan semua koset-koset dari I di R. Untuk setiap $a + I, b + I \in R/I$ didefinisikan:

1. $(a + I) + (b + I) = (a + b)I$
2. $(a + I)(b + I) = (ab) + I$

dengan $a, b \in R$. Dengan operasi ini, maka R/I disebut sebagai Ring Faktor atau *Quotient Ring.*

Contoh 2.12

Misalkan $(\mathbb{Z}, +, \cdot)$ adalah ring dengan $2\mathbb{Z}$ adalah ideal di $\mathbb{Z}$. Maka diperoleh ring faktor

$$\mathbb{Z}/2\mathbb{Z} = \{0 + 2\mathbb{Z},\ 1 + 2\mathbb{Z}\} = \{0, 1\}$$

dengan

$$(0 + 2\mathbb{Z}) + (0 + 2\mathbb{Z}) = (0 + 0) + 2\mathbb{Z} = 0 + 2\mathbb{Z}$$

$$(1 + 2\mathbb{Z}) + (1 + 2\mathbb{Z}) = (1 + 1) + 2\mathbb{Z} = 0 + 2\mathbb{Z}$$

$$(0 + 2\mathbb{Z}) + (1 + 2\mathbb{Z}) = (0 + 1) + 2\mathbb{Z} = 1 + 2\mathbb{Z}$$

$$(0 + 2\mathbb{Z}) \cdot (0 + 2\mathbb{Z}) = (0 \cdot 0) + 2\mathbb{Z} = 0 + 2\mathbb{Z}$$

$$(1 + 2\mathbb{Z}) \cdot (1 + 2\mathbb{Z}) = (1 \cdot 1) + 2\mathbb{Z} = 1 + 2\mathbb{Z}$$

$$(0 + 2\mathbb{Z}) \cdot (1 + 2\mathbb{Z}) = (0 \cdot 1) + 2\mathbb{Z} = 0 + 2\mathbb{Z}$$

2.1.4 Ring Noether

Definisi 2.13

Suatu ring *R* dengan elemen satuan dikatakan memenuhi syarat rantai naik (*ascending chain*) jika untuk sebarang rantai naik dari ideal-ideal di *R* terdapat bilangan bulat positif k sedemikian sehingga

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_k = I_{k+1} = I_{k+2}$$

Ring yang memenuhi syarat rantai naik pada idealnya disebut ring *Noether* (Persulessy & Dahoklory, 2015).

Contoh 2.13

Berdasarkan Contoh 2.9, $n\mathbb{Z}$ merupakan ideal di ring $\mathbb{Z}$. Untuk sebarang ideal $n_i\mathbb{Z}$, dengan $i = 1, 2, 3, \ldots, t$, pada ring $\mathbb{Z}$ selalu diperoleh rantai berikut

$$n\mathbb{Z} \subset n_1\mathbb{Z} \subset n_2\mathbb{Z} \subset \cdots \subset n_t\mathbb{Z}$$

dengan $n_1, n_2, \ldots, n_t$ adalah faktor pembagi n dan n_t adalah faktor prima terkecil. Sehingga $\mathbb{Z}$ memenuhi syarat rantai naik pada idealnya. Dengan demikian, ring $\mathbb{Z}$ merupakan ring *Noether*.

2.1.5 Tertutup secara Integral

Definisi 2.14

Misalkan S merupakan daerah integral dengan R adalah subring dari S, suatu $s \in S$ dikatakan integral atas R jika terdapat polinomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x^1 + a_0x^0$$

di $R[x]$ sedemikian sehingga berlaku

$$f(s) = s^n + a_{n-1}s^{n-1} + \cdots + a_1s^1 + a_0s^0 = 0$$

(Persulessy & Dahoklory, 2015).

Contoh 2.14

Daerah integral $\mathbb{Z}$ tertutup secara integral. Berikut akan ditunjukkan bahwa $\mathbb{Z}$ tertutup secara integral. Misalkan $x = \frac{p}{q} \in \mathbb{Q}$ dengan $r \in \mathbb{Q}$ integral atas $\mathbb{Z}$ di mana $\gcd(p, q) = 1$. Maka terdapat polinomial $f(x)$ di $\mathbb{Z}[x]$

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0x^0 + a_1x^1 + a_2x^2 + \cdots + x^n$$

dengan $i = 1, 2, 3, \ldots, n$. Untuk $x = \frac{p}{q} \in \mathbb{Q}$ yang integral atas $\mathbb{Z}$, maka

$$f\left(\frac{p}{q}\right) = \sum_{i=0}^{n} a_i \left(\frac{p}{q}\right)^i = a_0\left(\frac{p}{q}\right)^0 + a_1\left(\frac{p}{q}\right)^1 + a_2\left(\frac{p}{q}\right)^2 + \cdots + \left(\frac{p}{q}\right)^n$$

Sehingga diperoleh

$$f\left(\frac{p}{q}\right) = \sum_{i=0}^{n} a_i \left(\frac{p}{q}\right)^i$$

$$0 = \left(\frac{p}{q}\right)^n + \sum_{i=0}^{n-1} a_i \left(\frac{p}{q}\right)^i$$

$$\left(\frac{p}{q}\right)^n = -\left(\sum_{i=0}^{n-1} a_i \left(\frac{p}{q}\right)^i\right)$$

$$(p)^n = -\left(\sum_{i=0}^{n-1} a_i \left(\frac{p}{q}\right)^i\right) q^n = -\left(\sum_{i=0}^{n-1} a_i p^i q^{n-i-1}\right) q$$

Dengan demikian, diperoleh $q|p^n$. Karena $\gcd(p,q) = 1$ maka $q|p$ sehingga $\frac{p}{q} \in \mathbb{Z}$. Jadi $\mathbb{Z}$ tertutup secara integral di $\mathbb{Q}$.

2.1.6 Ring Dedekind

Ring Dedekind merupakan salah satu ring penting dalam aljabar yang memiliki banyak karakteristik dan kegunaan, salah satunya pada ilmu kriptografi (Jankowska & Matysiak, 2022). Ring Dedekind pertama kali diperkenalkan pada tahun 1879 oleh seorang matematikawan Jerman, Julius Wilhelm Richard Dedekind. Dalam aljabar abstrak, ring Dedekind adalah ring dengan setiap ideal tak nolnya dapat difaktorkan menjadi hasil kali dari ideal-ideal prima (Persulessy & Dahoklory, 2015).

Definisi 2.15

Ring D dikatakan ring Dedekind jika memenuhi kondisi berikut (Wijayanti, 2022):

1. D adalah ring *Noether*
2. D tertutup secara integral.
3. Setiap ideal prima tak nol dari D merupakan ideal maksimal

Contoh 2.15

Ring $\mathbb{Z}$ merupakan ring Dedekind, karena memenuhi kondisi berikut:

1. Pada Contoh 2.13, telah ditunjukkan bahwa ring $\mathbb{Z}$ merupakan ring *Noether*.
2. Pada contoh 2.14, telah ditunjukkan bahwa $\mathbb{Z}$ tertutup secara integral.
3. Akan ditunjukkan setiap ideal prima taknol di $\mathbb{Z}$ merupakan ideal maksimal.

Diketahui bahwa setiap ideal di $\mathbb{Z}$ berbentuk $n\mathbb{Z} = \langle n \rangle$. Misalkan $\langle p \rangle$ suatu ideal prima, maka p merupakan elemen prima. Selanjutnya misalkan terdapat $\langle r \rangle$ dengan $\langle p \rangle \subseteq \langle r \rangle$. Karena $\mathbb{Z}$ merupakan daerah integral utama, maka $r|p$ yang berarti r merupakan salah satu faktor dari p. Sehingga terdapat dua kondisi yaitu r merupakan unit atau r berasosiasi dengan p:

a. Jika r unit maka diperoleh

$$\langle r \rangle = \mathbb{Z}$$

b. Jika r berasosiasi dengan p, maka $p = ur$ dengan u unit sehingga diperoleh

$$\langle r \rangle = \langle p \rangle$$

Dengan demikian $\langle p \rangle$ merupakan ideal maksimal karena ideal $\langle p \rangle$ hanya termuat dalam $\langle p \rangle$ dan $\mathbb{Z}$.

2.1.7 Fungsi Euler untuk Ideal pada Ring Dedekind

Definisi 2.16

Misalkan R adalah ring Dedekind dan I adalah ideal dari ring R. R/I merupakan ring faktor yang dibentuk dari ideal I dalam ring R. Fungsi Euler untuk ideal pada ring Dedekind didefinisikan sebagai berikut (Petukhova & Tronin, 2016):

$$\phi(I) = |U(R/I)|$$

dengan $U(R/I)$ adalah grup dari unit. Selanjutnya, untuk setiap ideal maksimal M di R, jika $I = M_1.M_2.\ldots.M_m$ maka

$$\phi(I) = \prod_{i=1}^{m} \phi(M_i)$$

dengan $i = 1, 2, 3, \ldots, m$.

2.1.8 Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu *Crypto* yang berarti rahasia, dan *Graphia* yang berarti tulisan. Secara terminologi, kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan yang dikirim dari satu pihak ke pihak lain (Mukhtar, 2018). Kriptografi merupakan ilmu sekaligus seni mengenai teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti tingkat kenyamanan, integritas data, autentikasi entitas, serta identifikasi keaslian data (Menezes et al., 1996). Dengan kriptografi, pesan akan diacak menjadi pesan yang tidak bermakna sehingga pesan hanya dapat dipahami oleh pihak yang dituju.

Kriptografi menggunakan ilmu matematika dalam proses enkripsi dan dekripsi pesan. Enkripsi merupakan proses mengacak suatu pesan asli (plainteks) menjadi pesan acak (cipherteks) dengan kunci (*key*) yang telah disepakati oleh pengirim dan penerima pesan. Cipherteks kemudian dikirimkan kepada penerima pesan dan hanya dapat dipecahkan oleh penerima yang dituju. Selanjutnya penerima akan mengembalikan cipherteks yang diterima menjadi plainteks dengan kunci yang telah disepakati. Proses ini disebut dengan proses dekripsi. Hal ini berarti bahwa kriptografi bukan untuk menyembunyikan pesan melainkan untuk menyembunyikan makna dari pesan tersebut.

Tujuan utama dari kriptografi adalah menjaga keamanan pesan. Menurut Rinaldi Munir (2018), keamanan mencakup beberapa hal sebagai berikut:

1. *Confidentiality* atau kerahasiaan yaitu menjaga pesan agar tidak dapat dibaca ataupun dipahami oleh pihak yang tidak berkepentingan.

2. *Authentication* yang berarti pihak-pihak yang berkomunikasi harus dapat saling mengidentifikasi sehingga dapat memastikan kebenaran sumber pesan.
3. *Data integrity* (integritas data) yaitu menjamin bahwa pesan adalah pesan asli dan tidak dimanipulasi (mengalami perubahan) selama pengiriman.
4. *Non repudiation* yang berarti mencegah pihak yang saling berkomunikasi melakukan penyangkalan, baik pengirim menyangkal telah mengirim pesan maupun penerima menyangkal telah menerima pesan.

Algoritma kriptografi merupakan urutan atau langkah-langkah untuk menyelesaikan masalah yang disusun secara sistematis dalam menyembunyikan pesan dari pihak yang tidak berhak menerima pesan. Kekuatan suatu algoritma kriptografi bergantung dengan banyaknya usaha yang dibutuhkan pada proses enkripsi dan dekripsi pesan. Semakin banyak usaha yang dilakukan maka semakin lama pula waktu yang dibutuhkan. Hal ini berarti semakin tinggi pula kekuatan dari suatu algoritma kriptografi (Munir, 2016). Berdasarkan kunci yang digunakan, algoritma kriptografi dibagi menjadi tiga yaitu:

1. Algoritma Simetri

   Algoritma simetri merupakan algoritma kriptografi di mana kunci yang digunakan pada proses enkripsi dan dekripsi adalah sama. Tingkat keamanan dari algoritma ini terletak pada kunci yang digunakan, sehingga pengirim dan penerima harus membuat kunci yang berbeda setiap bertukar pesan. Pada algoritma simetri, keamanan pengiriman kunci perlu diperhatikan karena cipherteks dapat didekripsi oleh setiap pihak yang mengetahui kuncinya. Salah satu metode yang dianggap paling aman untuk menyepakati kunci ini

adalah dengan bertemu secara langsung. Hal inilah yang menjadi kelemahan dari algoritma klasik (Mukhtar, 2018).

2. Algoritma Asimetri

Algoritma asimetri disebut juga dengan algoritma kunci publik (*public key cryptosystem*). Konsep mengenai kriptografi kunci publik ini telah ditemukan oleh James Ellis pada tahun 1970an, di mana kunci kriptografi yang digunakan ada dua yaitu kunci publik dan kunci privat. Kunci publik digunakan dalam proses enkripsi sedangkan kunci privat digunakan untuk proses dekripsi pesan (Kraft & Washington, 2016). Kunci publik dapat diketahui oleh siapapun karena cipherteks tidak dapat didekripsi hanya dengan kunci publik. Kunci privat penerima juga tidak perlu dikirimkan kepada pengirim pesan, sehingga pesan hanya dapat didekripsi oleh penerima yang dituju.

3. *Hash Function*

Fungsi *hash* merupakan suatu fungsi matematika yang mengambil masukan panjang variabel dan mengubahnya menjadi urutan biner dengan panjang yang tepat. Fungsi *hash* disebut juga sebagai fungsi satu arah, *message digest, fingerprint,* dan *Message Authentication Code* (MAC). Fungsi ini diperlukan untuk membuat sidik jari atau tanda tangan digital pada pesan yang menandakan bahwa pesan tersebut asli (Ariyus, 2008).

Konsep mengenai penyandian pesan rahasia telah digunakan selama berabad abad dan dengan cara yang berbeda-beda. Bangsa Mesir, kurang lebih 4000 tahun lalu, menggunakan *hieroglyph* untuk menulis pesan di dinding piramid. Selanjutnya di Yunani, kriptografi dilakukan dengan menggunakan alat yang diberi nama *scytale.* Ilmu mengenai kriptografi ini terus berkembang seiring

dengan berjalannya waktu. Berdasarkan sejarahnya, kriptografi dibagi menjadi dua yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik dilakukan sebelum adanya komputer, sehingga hanya menggunakan pensil dan kertas. Algoritma yang digunakan berupa algoritma klasik di mana penyandian dilakukan untuk setiap karakter pesan. Selanjutnya, kriptografi modern diciptakan untuk meningkatkan keamanan dari konsep kriptografi. Algoritma kriptografi modern dibuat lebih kompleks agar cipherteks sulit untuk dipecahkan tanpa mengetahui kuncinya (Munir, 2006).

2.1.9 Algoritma RSA

Algoritma RSA merupakan salah satu kriptografi kunci publik yang paling banyak digunakan. Pada tahun 1977, Ron Rivest, Adi Shamir, dan Leonhard Adleman menemukan modifikasi dari kriptografi kunci publik yang kemudian dikenal sebagai algoritma RSA. Penelitian ini memiliki pengaruh yang sangat besar dalam perkembangan teori bilangan. Algoritma RSA menunjukkan bahwa teori bilangan, yang telah lama dianggap hanya sebagai cabang teori dari matematika murni, memiliki kegunaan yang penting (Kraft & Washington, 2016). Misalnya, karena keamanan dari sistem RSA berkaitan erat dengan sulitnya pemfaktoran, pengembangan atas algoritma pemfaktoran mendapat banyak perhatian dan masalah komputasi menjadi lebih populer. Secara umum, algoritma RSA menunjukkan fakta bahwa cukup mudah untuk mengalikan dua bilangan prima besar, namun sulit untuk memfaktorkan bilangan ke faktor primanya dengan efisien (Hodge et al., 2013).

Proses enkripsi dan dekripsi pada algoritma RSA menggunakan dua kunci, yaitu kunci publik dan kunci privat. Kunci publik yang merupakan hasil

kali dua bilangan prima besar digunakan untuk proses enkripsi, sedangkan kunci privat digunakan untuk proses dekripsi oleh penerima pesan (Munir, 2016). Berikut ini merupakan langkah-langkah penyandian pesan menggunakan algoritma RSA dengan Alice dan Bob sebagai dua pihak yang akan berkomunikasi:

1. Proses Pembangkitan dan Pembentukan Kunci
    a. Alice, sebagai penerima pesan, memilih dua bilangan prima besar yaitu p dan q, selanjutnya menghitung nilai n yang merupakan hasil kali dari dua bilangan prima
    $$n = pq$$
    b. Alice menghitung $\phi(n) = (p-1)(q-1)$. Nilai $\phi(n)$ harus dirahasiakan karena berkaitan dengan proses dekripsi.
    c. Alice memilih kunci enkripsi e di mana $\gcd(e, \phi(n)) = 1$.
    d. Alice menghitung bilangan bulat positif d, yang kemudian disebut sebagai kunci dekripsi, dengan $ed \equiv 1 \pmod{\phi(n)}$.
    e. Alice mempublikasikan n dan e dan merahasiakan nilai $d, p,$ dan q. Sehingga dari proses ini diperoleh kunci publik (n, e) dan kunci privat (p, q, d).
2. Proses Enkripsi Pesan dengan RSA
    a. Bob, sebagai pengirim pesan, menerima kunci publik n dan e.
    b. Bob menulis pesan m di mana $0 < m < n$. Jika nilai m lebih besar dari n, maka m perlu dibagi menjadi beberapa blok sehinga m kurang dari n.
    c. Bob melakukan enkripsi dengan melakukan enkripsi dengan persamaan

$$c \equiv m^e \pmod{n}$$

kemudian mengirimkan hasil enkripsi kepada Alice.

3. Proses Dekripsi Pesan dengan RSA
   a. Alice menerima cipherteks c dari Bob
   b. Alice mendekripsi pesan dengan

$$m \equiv c^d \pmod{n}$$

Rumus dekripsi tersebut dapat mengembalikan pesan sesuai dengan pesan asli merupakan akibat dari teorema Euler yang ditujukkan dalam teorema berikut:

Teorema 2.7

Misalkan $n = pq$ adalah hasil kali dari dua bilangan prima besar dan misalkan d dan e memenuhi $ed \equiv 1 \big(\mathrm{mod}\ (p-1)(q-1)\big)$. Maka untuk semua bilangan bulat m berlaku

$$m^{ed} \equiv m \pmod{n}$$

Oleh karena itu, jika $c \equiv m^e \pmod{n}$ maka $m \equiv c^d \pmod{n}$

Bukti:

Pembuktian akan dibagi dalam beberapa kasus:

Kasus 1: untuk $\gcd(m, n) = 1$. Diketahui bahwa $ed \equiv 1 \pmod{\phi(n)}$ atau dapat ditulis sebagai

$$ed = 1 + \ k \cdot \phi(n) = 1 + k\big((p-1)(q-1)\big)$$

untuk sebarang nilai k. Dengan teorema Euler berikut,

$$m^{\phi(n)} \equiv 1(mod\ n)$$

maka diperoleh,

$$m^{ed} \equiv m^{1+\ k.\phi(n)} \equiv m(m^{\phi(n)})^k \equiv m(1)^{\ k} \equiv m \pmod{n}$$

Selanjutnya perlu untuk dibuktikan untuk kasus di mana $\gcd(m,n) > 1$. Telah diketahui bahwa n adalah hasil kali dari dua bilangan prima besar p dan q. Dengan demikian $\gcd(m,n)$ adalah pembagi dari $n = pq$, maka haruslah $\gcd(m,n) = p, q,$ atau pq

Kasus 2: untuk $\gcd(m,n) = pq$. Pada kasus ini terlihat bahwa $n|m$ sehingga

$$m \equiv 0 \ (mod\ n)$$

Dengan demikian diperoleh,

$$m^{ed} \equiv 0^{ed} \equiv 0 \equiv m \ (\text{mod}\ n)$$

Kasus 3: akan dibuktikan untuk $\gcd(m,n) = p$ dan $\gcd(m,n) = q$. Asumsikan bahwa $\gcd(m,n) = p$. Hal ini berarti bahwa $p|m$ sehingga

$$m \equiv 0 \ (mod\ p)$$

Dengan demikian diperoleh,

$$m^{ed} \equiv 0^{ed} \equiv 0 \equiv m \ (\text{mod}\ p)$$

Perlu diperhatikan bahwa $q \nmid m$ maka $m \not\equiv 0 \ (mod\ q)$, dengan teorema Fermat diperoleh,

$$m^{q-1} \equiv 1 \ (mod\ q)$$

Oleh karena itu,

$$m^{ed} \equiv m^{1+\,k.(p-1)(q-1)} \equiv m(m^{(q-1)})^{k(p-1)} \equiv m(1)^{\,k(p-1)} \equiv m \ (\text{mod}\ q)$$

Dengan demikian, telah dibuktikan bahwa $p|m^{ed} - m$ dan $q|m^{ed} - m$. Sehingga $pq|m^{ed} - m$ yang berarti bahwa $m^{ed} \equiv m \ (\text{mod}\ pq) \equiv m \ (\text{mod}\ n)$. Hal ini juga berlaku untuk $\gcd(m,n) = q$. ■

Pada algoritma RSA, kunci enkripsi berupa kunci publik sehingga dapat diketahui umum sedangkan kunci dekripsi bersifat rahasia. Untuk menemukan kunci dekripsi, perlu dilakukan pemfaktoran bilangan non prima menjadi faktor

primanya. Kekuatan algoritma RSA terletak pada sulitnya memfaktorkan bilangan menjadi faktor primanya. Oleh karena itu, semakin besar bilangan prima maka semakin sulit pula pemfaktorannya. Semakin sulit pemfaktoran maka berarti semakin tinggi pula tingkat keamananya. Algoritma RSA banyak direkomendasikan untuk penyandian pesan karena belum ditemukan algoritma yang paling efisien untuk memfaktorkan bilangan bulat menjadi faktor primanya (Munir, 2016).

2.2 Kajian Integrasi Topik dengan Al-Qur'an/Hadist

Al-Qur'an merupakan wahyu yang diturunkan kepada Rasulullah Muhammad SAW sebagai pedoman hidup bagi umat Islam. Melalui Al-Qur'an, Allah SWT memberikan petunjuk bagi seluruh umat-Nya mengenai berbagai hal, termasuk perintah untuk menyampaikan amanat yang berkaitan dengan Allah SWT dan sesama manusia dengan jujur. Secara bahasa, amanah berasal dari kata *amina –ya'manu – amnan – amanatan* yang berarti jujur atau dapat dipercaya. Amanah juga dapat berarti titipan (Munawwir, 1984). Titipan disini yaitu segala sesuatu yang harus disampaikan kepada pihak yang berhak menerimanya. Amanah secara terminologi berarti segala sesuatu yang dipertanggungjawabkan kepada orang lain.

Dalam Al-Qur'an terdapat beberapa surah mengenai perintah menyampaikan amanat, salah satunya adalah dalam Surah An-Nisa' ayat 58 sebagai berikut (Lajnah Pentashihan Mushaf Al-Qur'an, 2018):

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 ﴿٥٨﴾

Artinya: *"Sesungguhnya Allah SWT menyuruh kamu menyampaikan amanah kepada pemiliknya. Apabila kamu menetapkan hukum di antara manusia, hendaklah kamu tetapkan secara adil. Sesungguhnya Allah Maha Mendengar lagi Maha Melihat".*

Dalam ayat ini, Allah SWT memerintahkan untuk menyampaikan amanat kepada yang berhak menerima. Amanat merupakan segala sesuatu yang dipercayakan kepada seseorang untuk dilaksanakan sebaik-baiknya. Kata amanat disini memiliki arti yang sangat luas, yaitu baik amanat kepada Allah, kepada sesama manusia, maupun kepada diri sendiri. Amanat kepada sesama manusia di antaranya adalah mengembalikan titipan kepada pemiliknya tanpa adanya pengurangan maupun penambahan, tidak menipu, memelihara rahasia, dan lain sebagainya. Termasuk pula didalamnya yaitu sifat adil, dengan tidak membeda-bedakan antara satu dengan yang lain, dalam menetapkan hukum (Kemenag, 2019).

Berdasarkan Tafsir Ibnu Katsir (2008), dalam ayat

۞ اِنَّ اللّٰهَ يَأْمُرُكُمْ اَنْ تُؤَدُّوا الْاَمٰنٰتِ اِلٰٓى اَهْلِهَاۙ

Allah SWT memberitahukan bahwa Dia memerintahkan agar amanat disampaikan kepada yang berhak menerimanya. Dalam hadits yang diriwayatkan oleh Abu Dawud, disebutkan bahwa Rasulullah SAW bersabda:

حَدَّثَنَا مُحَمَّدُ بْنُ الْعَلَاءِ وَأَحْمَدُ بْنُ إِبْرَاهِيمَ قَالَا حَدَّثَنَا طَلْقُ بْنُ غَنَّامٍ عَنْ شَرِيكٍ قَالَ ابْنُ الْعَلَاءِ وَقَيْسٌ عَنْ أَبِي حُصَيْنٍ عَنْ أَبِي صَالِحٍ عَنْ أَبِي هُرَيْرَةَ قَالَ قَالَ رَسُولُ اللَّهِ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ أَدِّ الْأَمَانَةَ إِلَى مَنْ ائْتَمَنَكَ وَلَا تَخُنْ مَنْ خَانَكَ

Artinya: *"Sampaikanlah amanat itu kepada orang yang mempercayaimu, dan janganlah kamu berkhianat terhadap orang yang berkhianat kepadamu"*.

Makna amanat dalam hadis ini bersifat umum yang mencakup semua jenis amanat yang diharuskan bagi manusia untuk menyampaikannya. Amanat tersebut di antaranya yaitu amanat yang menyangkut hak-hak Allah, seperti shalat, zakat, puasa, kafarat, nazar, dan lain sebagainya. Secara umum, amanat yang menyangkut hak-hak Allah ini berupa perintah untuk senantiasa beribadah kepada-Nya dan

menjauhi larangan-Nya, sebagaimana yang tertuang dalam surah Az Zariyat ayat 56 berikut (Lajnah Pentashihan Mushaf Al-Qur'an, 2018):

وَمَا خَلَقْتُ الْجِنَّ وَالْاِنْسَ اِلَّا لِيَعْبُدُوْنِ ﴿٥٦﴾

Artinya: *"Tidaklah Aku menciptakan jin dan manusia kecuali untuk beribadah kepada-Ku"*.

Melalui ayat ini, Allah memerintahkan Nabi Muhammad SAW untuk beristiqamah dan mengajak umat-Nya untuk mengagungkan-Nya, karena sesungguhnya itulah tujuan dari penciptaan manusia.

Selanjutnya, amanah yang berkaitan dengan hak-hak hamba yaitu segala titipan, baik berupa benda, perkataan, perbuatan, maupun kepercayaan. Maka Allah SWT memerintahkan agar hak-hak tersebut ditunaikan kepada yang berhak menerimanya, karena barangsiapa yang tidak melakukan hal tersebut di dunia maka ia akan dituntut pada hari kiamat dan dihukum karenanya. Sufyan As Sauri meriwayatkan dari Ibnu Abu Laila, dari seorang lelaki, dari Ibnu Abbas mengenai makna amanat dalam surah An Nisa ayat 58 ini, yaitu amanat bermakna umum dan wajib ditunaikan terhadap semua orang, baik yang bertaqwa maupun yang tidak.

Allah SWT melarang umat-Nya mengkhianati amanat, karena amanat erat kaitannya dengan kepercayaan. Apabila amanat tidak lagi terpelihara maka kepercayaan akan hilang, sehingga berakibat ketenangan hidup dalam bermasyarakat tidak dapat lagi dirasakan. Kebalikan dari sifat amanah ini adalah khianat. Khianat merupakan sifat orang-orang munafik yang dapat mengikis habis iman seorang mukmin. Dalam hadits yang diriwayatkan oleh Imam Bukhari, disebutkan tiga tanda orang yang munafiq yaitu sebagai berikut (Abdul Baqi, 2017):

حَدَّثَنَا سُلَيْمَانُ أَبُو الرَّبِيعِ قَالَ حَدَّثَنَا إِسْمَاعِيلُ بْنُ جَعْفَرٍ قَالَ حَدَّثَنَا نَافِعُ بْنُ مَالِكِ بْنِ أَبِي عَامِرٍ أَبُو سُهَيْلٍ عَنْ أَبِيهِ عَنْ أَبِي هُرَيْرَةَ عَنْ النَّبِيِّ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ قَالَ آيَةُ الْمُنَافِقِ ثَلَاثٌ إِذَا حَدَّثَ كَذَبَ وَإِذَا وَعَدَ أَخْلَفَ وَإِذَا اؤْتُمِنَ خَانَ

Artinya: *"Tanda-tanda munafiq ada tiga yaitu jika berbicara dusta, jika berjanji mengingkari, dan jika diberi amanat dia khianat"*

Selanjutnya, Allah SWT berfirman

وَاِذَا حَكَمْتُمْ بَيْنَ النَّاسِ اَنْ تَحْكُمُوْا بِالْعَدْلِۗ اِنَّ اللّٰهَ نِعِمَّا يَعِظُكُمْ بِهٖۗ اِنَّ اللّٰهَ كَانَ سَمِيْعًاۢ بَصِيْرًا ﴿٥٨﴾

Ayat ini merupakan perintah Allah SWT yang menganjurkan untuk menetapkan hukum di antara manusia dengan adil. Dalam sebuah hadits disebutkan bahwa, sesungguhnya Allah SWT selalu bersama hakim selama ia tidak bersikap zalim, dan apabila berbuat zalim dalam keputusannya, maka Allah SWT menyerahkan dia kepada dirinya sendiri (atau menjauh darinya). Sesungguhnya Allah SWT Maha mendengar segala ucapan dan Maha melihat segala perbuatan makhluk-Nya.

Secara umum, dalam surah An Nisa ayat 58 ini Allah memerintahkan untuk menyampaikan amanat-amanat tersebut diatas dan memutuskan hukum dengan adil di antara manusia serta lain-lainnya termasuk perintah-Nya dan syariat-Nya yang sempurna lagi agung (Ibnu Katsir, 2008).

Hal ini sesuai dengan konsep kriptografi yaitu menjaga keamanan pesan. Pesan akan disandikan dengan algoritma kriptografi sehingga pesan hanya dapat dipahami oleh penerima yang dituju. Dengan demikian, pesan dapat sampai kepada penerima sesuai dengan isi sebenarnya tanpa adanya perubahan yang dilakukan oleh pihak yang tidak bertanggung jawab. Melalui kriptografi, pihak yang berkomunikasi dapat mengidentifikasi satu sama lain sehingga kebenaran sumber pesan dapat terjamin. Kriptografi juga dapat mencegah pihak yang berkomunikasi

melakukan penyangkalan, baik penerima menyangkal telah menerima pesan ataupun pengirim menyangkal telah mengirim pesan.

2.3 Kajian Topik dengan Teori Pendukung

Kriptografi merupakan salah satu metode yang dapat digunakan untuk meningkatkan keamanan pada proses bertukar pesan atau data, sehingga pesan dapat diterima oleh pihak yang dituju tanpa adanya perubahan. Dalam ilmu kriptografi, terdapat beberapa algoritma kriptografi yang dapat digunakan untuk menyandikan pesan, salah satunya yaitu algoritma RSA. Algoritma ini memiliki pengaruh yang besar terhadap perkembangan teori bilangan dengan menunjukkan bahwa teori bilangan tidak hanya sebagai cabang dalam matematika murni, namun juga memiliki kegunaan yang nyata. Algoritma RSA ini menggunakan dua kunci yang berbeda, yaitu kunci publik yang merupakan hasil kali dua bilangan prima besar dan kunci privatnya berupa dua bilangan prima besar yang hanya diketahui oleh penerima pesan. Semakin besar bilangan prima yang digunakan maka semakin semakin sulit pemfaktorannya, yang berarti semakin tinggi pula tingkat keamanannya. Proses penyandian pesan dengan algoritma ini pada dasarnya dibagi menjadi tiga bagian, yaitu proses pembentukan kunci, proses enkripsi, dan proses dekripsi. Proses penyandian pesan ini erat kaitannya dengan konsep kongruensi dan keterbagian. Selanjutnya, pada penelitian ini algoritma RSA akan diimplementasikan pada ring Dedekind. Pasangan bilangan prima pada proses pembentukan kunci diganti dengan ideal-ideal pada ring Dedekind dan fungsi Euler yang digunakan adalah fungsi Euler untuk ideal pada ring Dedekind. Dengan demikian pada penelitian ini diperlukan teori pendukung mengenai ring, ideal, dan fungsi Euler.

BAB III
METODE PENELITIAN

3.1 Jenis Penelitian

Jenis penelitian yang digunakan dalam penelitian ini adalah penelitian kualitatif. Penelitian ini bertujuan untuk mengembangkan ide-ide baru, wawasan atau bahkan teori baru melalui referensi dan hasil penelitian yang berkaitan dengan bidang ilmu. Data dan informasi yang digunakan dalam penelitian ini diambil dari beberapa sumber literatur seperti buku, jurnal, artikel, laporan hasil penelitian, dan lain sebagainya yang mendukung penelitian ini.

3.2 Pra Penelitian

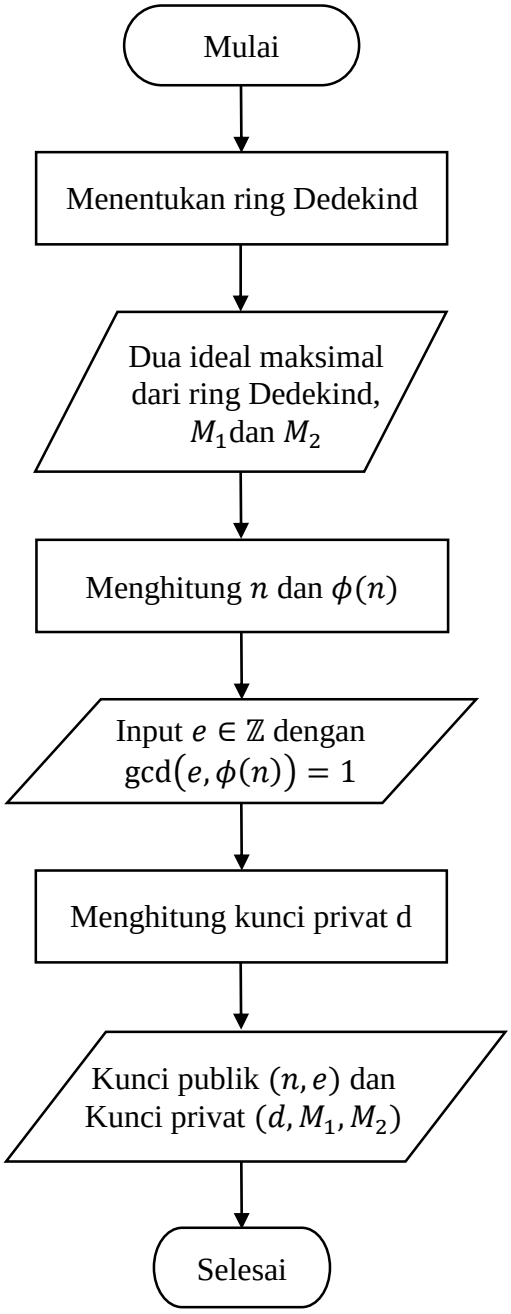
Pra penelitian yang dilakukan dalam penelitian ini adalah mencari dan mempelajari beberapa referensi penelitian, seperti jurnal, artikel, buku, dan referensi-referensi lain sebagai sumber rujukan dalam menentukan topik penelitian. Selanjutnya, peneliti mengumpulkan beberapa literatur yang berkaitan dengan teori pendukung dan pembahasan, terutama mengenai algoritma RSA dan algoritma kriptografi atas ring Dedekind.

3.3 Tahapan Penelitian

Penelitian ini memiliki tiga tahapan yaitu proses pembentukan kunci, proses enkripsi, dan proses dekripsi. Berikut langkah-langkah yang digunakan dalam tahapan penelitian algoritma RSA atas ring Dedekind:

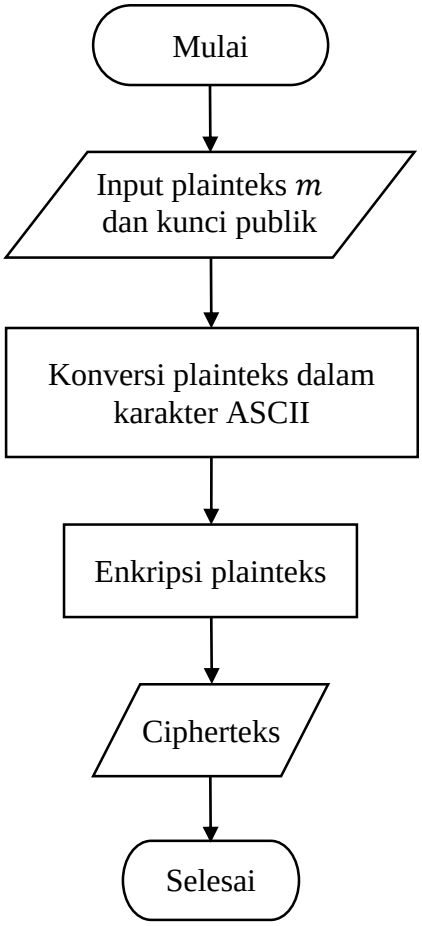
1. Proses pembentukan kunci pada algoritma RSA atas ring Dedekind:
    a. Menentukan ring Dedekind D yang digunakan dan ideal maksimal $M_1, M_2 \in D$ dengan $M_1 \neq M_2$

b. Melakukan pembentukan kunci pada algoritma RSA atas ring Dedekind sehingga diperoleh pasangan kunci publik dan kunci privat yang selanjutnya digunakan pada proses enkripsi dan dekripsi pesan.



Gambar 3.1 *Flowchart* Proses Pembentukan Kunci

2. Mengonstruksi algoritma enkripsi dengan RSA atas ring Dedekind sebagai berikut:
   a. Menentukan plainteks yang akan dienkripsi kemudian mengkonversi plainteks sesuai dengan ASCII *printable character*.
   b. Melakukan enkripsi plainteks dengan mensubtitusikan plainteks dan kunci publik yang telah ditentukan ke dalam persamaan enkripsi RSA atas ring Dedekind sehingga diperoleh pesan yang telah disandikan atau cipherteks berupa angka yang selanjutnya dikirimkan kepada penerima pesan untuk didekripsi.

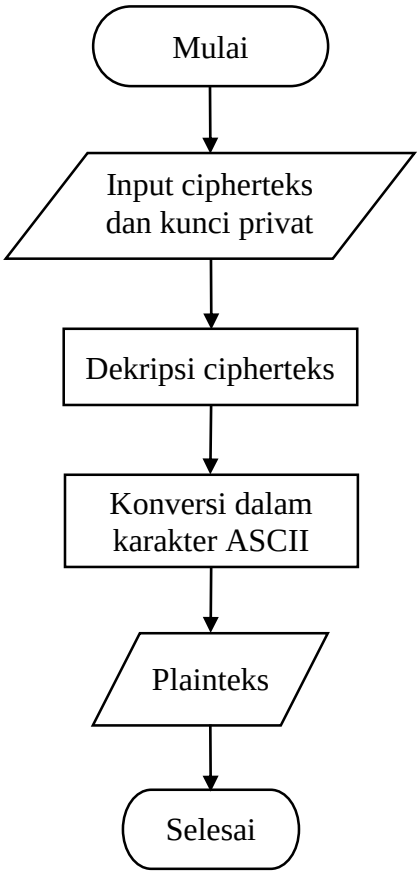


Gambar 3.2 *Flowchart* Algortima Enkripsi RSA atas Ring Dedeknd

3. Mengonstruksi algoritma dekripsi dengan RSA atas ring Dedekind sebagai berikut:

a. Melakukan dekripsi pesan dengan mensubtitusikan cipherteks dan kunci privat yang telah ditentukan ke dalam persamaan dekripsi RSA atas ring Dedekind.

b. Mengkonversi hasil dekripsi ke dalam bentuk karakter berdasarkan ASCII *printable characters.* Sehingga diperoleh plainteks hasil dekripsi yang sesuai dengan plainteks awal.



Gambar 3.3 *Flowchart* Algoritma Dekripsi RSA atas Ring Dedekind

BAB IV
HASIL DAN PEMBAHASAN

4.1 Proses Pembentukan Kunci Algoritma RSA atas Ring Dedekind

Algoritma RSA merupakan salah satu algoritma kriptografi yang memanfaatkan kunci yang berbeda dalam mengamankan pesan. Penerima pesan membangkitkan dua kunci yang berbeda yaitu kunci publik dan kunci privat. Selanjutnya kunci publik akan dikirimkan kepada Pengirim pesan untuk digunakan dalam proses enkripsi, sedangkan kunci privat akan digunakan untuk proses dekripsi pesan. Kunci yang digunakan dalam proses enkripsi algoritma RSA berupa hasil kali dari dua bilangan prima besar, sehingga keamanan dari algoritma ini bergantung pada tingkat kesulitan pemfaktoran hasil perkalian bilangan prima tersebut.

Seiring dengan berkembangnya ilmu pengetahuan, telah dilakukan beberapa penelitian mengenai modifikasi algoritma kriptografi, termasuk algoritma RSA, dengan tujuan untuk meningkatkan tingkat keamaan penyandian pesan. Pada penelitian ini membahas mengenai implementasi algoritma kriptografi RSA atas ring Dedekind. Ring Dedekind merupakan salah satu ring penting dalam aljabar yang memiliki banyak karakteristik dan kegunaan, salah satunya dalam kriptografi. Suatu ring dikatakan Dedekind jika tertutup secara integral, berupa ring *noetherian*, dan setiap ideal tak nolnya adalah ideal maksimal. Pada algoritma ini, ring Dedekind akan berperan penting dalam proses penyandian pesan terutama pada pembentukan kunci untuk memperoleh kunci publik dan kunci privat.

4.1.1 Algoritma Pembentukan Kunci

Pada algoritma kriptografi kunci publik, proses pembentukan kunci dilakukan oleh penerima pesan. Penerima membentuk dua pasang kunci yaitu kunci publik yang selanjutnya dikirimkan kepada pengirim pesan, dan kunci privat yang disimpan untuk proses dekripsi pesan. Pada proses pembentukan kunci algoritma RSA atas ring Dedekind, penerima pesan menentukan ring Dedekind yang akan digunakan terlebih dahulu. Selanjutnya, pasangan bilangan prima dalam proses pembentukan kunci akan diganti dengan ideal-ideal maksimal dari ring Dedekind tersebut. Sehingga kunci publik yang digunakan diperoleh dari hasil kali dari dua ideal maksimal yang berbeda dari ring Dedekind. Fungsi Euler yang digunakan adalah fungsi Euler untuk ideal pada ring Dedekind yang berupa hasil kali dari kardinalitas grup unit.

Berikut ini merupakan algoritma proses pembentukan kunci dengan menggunakan algoritma RSA atas ring Dedekind:

1. Menentukan ring Dedekind D yang akan digunakan.
2. Menentukan dua ideal maksimal berbeda yaitu M_1 dan M_2 dari ring Dedekind D.
3. Menghitung nilai n yang diperoleh dari hasil kali dari dua ideal maksimal dari ring Dedekind D yang telah ditentukan, atau dapat dituliskan sebagai berikut:

   $$N = M_1.M_2 \tag{4.1}$$

   Sehingga diperoleh himpunan N yang merupakan himpunan bilangan hasil kali dari dua ideal maksimal. Selanjutnya dipilih sebarang $n \in N$ di mana

$n > 0$ untuk dijadikan sebagai kunci publik. Semakin besar nilai n yang dipilih maka semakin sulit pula pemfaktorannya.

4. Menentukan fungsi Euler $\phi(N)$ untuk ideal pada ring Dedekind sesuai dengan Definisi 2.16 yaitu berupa hasil kali dari kardinalitas grup unit

$$\phi(N) = |U(R/M_1)|.|U(R/M_2)| \tag{4.2}$$

5. Menentukan sebarang bilangan bulat e sebagai kunci publik yang relatif prima terhadap $\phi(N)$ yaitu dengan $\gcd\big(e, \phi(N)\big) = 1$
6. Dengan demikian, penerima pesan memperoleh pasangan kunci publik (n, e) yang selanjutnya dikirimkan kepada pengirim pesan untuk proses enkripsi pesan.
7. Selanjutnya akan dihitung kunci privat d yang digunakan pada proses dekripsi pesan dengan kekongruenan

$$ed \equiv 1(mod\ \phi(N)) \tag{4.3}$$

Berdasarkan Teorema 2.4, $ed \equiv 1(mod\ \phi(N))$ ekuivalen dengan $ed = 1 + k.\varphi(N)$ sehingga d dapat dihitung dengan persamaan berikut:

$$d = \frac{1 + k.\phi(N)}{e} \tag{4.4}$$

dengan $k \in \mathbb{Z}^+$. Dengan demikian diperoleh nilai d sebagai kunci dekripsi yang dirahasiakan.

8. Memperoleh kunci rahasia (d, M_1, M_2) yang hanya diketahui oleh penerima pesan untuk proses dekripsi pesan.

4.1.2 Simulasi Pembentukan Kunci

Berikut merupakan simulasi pembentukan kunci publik dan kunci privat dengan algoritma RSA atas ring Dedekind:

1. Menentukan ring Dedekind D yang akan digunakan. Pada simulasi ini, dipilih ring Dedekind berupa ring bilangan bulat $\mathbb{Z}$. Pada Contoh 2.15 telah dibuktikan bahwa ring $\mathbb{Z}$ memenuhi syarat ring Dedekind yaitu merupakan ring *Noether,* tertutup secara integral, dan setiap ideal prima tak nol dari $\mathbb{Z}$ merupakan ideal maksimal.
2. Menentukan dua ideal maksimal yang berbeda yaitu M_1 dan M_2 dari ring $\mathbb{Z}$. Dipilih $M_1 = \langle 11 \rangle = 11\mathbb{Z}$ dan $M_2 = \langle 13 \rangle = 13\mathbb{Z}$. Selanjutnya akan dibuktikan bahwa M_1 dan M_2 merupakan ideal maksimal dari ring $\mathbb{Z}$.

   Misalkan $\mathbb{Z}$ adalah ring bilangan bulat dan P merupakan ideal di $\mathbb{Z}$. Jika $P = \langle p \rangle$ untuk setiap $p \in \mathbb{Z}$ adalah bilangan prima, maka P adalah ideal maksimal di $\mathbb{Z}$.

   Bukti:

   Diketahui P merupakan ideal di $\mathbb{Z}$. Misalkan M adalah ideal maksimal di $\mathbb{Z}$, maka $P \subset M$. Karena M adalah suatu ideal di $\mathbb{Z}$ maka $M = \langle n\mathbb{Z} \rangle$ dengan $n\mathbb{Z} \in \mathbb{Z}$. Misalkan $p \in P$ berarti $p = m.n\mathbb{Z}$ untuk setiap $m \in \mathbb{Z}$ karena $p \in P \subset M$. Jika p prima, maka berakibat $n\mathbb{Z} = 1$ atau $n\mathbb{Z} = p$.

   a. Jika $n\mathbb{Z} = p$ maka $n\mathbb{Z} \in P$. Berarti $M \subset P$, sehingga $M = P$.
   b. Jika $n\mathbb{Z} = 1$ maka $1 \in \mathbb{Z}$. Ambil sebarang $x \in \mathbb{Z}$ sedemikian sehingga $1.x = x \in \mathbb{Z}$, maka $\mathbb{Z} \subset M$ dan $M \subset \mathbb{Z}$. Hal ini berarti $M = \mathbb{Z}$.

   Dengan demikian diperoleh $M = \mathbb{Z}$ dan $P \subset M$. Berdasarkan Definisi 2.11 mengenai ideal maksimal maka P adalah ideal maksimal di $\mathbb{Z}$.
3. Menghitung nilai n dengan mensubtitusi ideal-ideal maksimal yang telah ditentukan sebelumnya ke persamaan (4.1), sehingga diperoleh sebagai berikut:

$$N = M_1 . M_2$$
$$= 11\mathbb{Z} . 13\mathbb{Z}$$
$$= 143\mathbb{Z}$$

Dengan demikian diperoleh himpunan hasil kali ideal maksimal yaitu $N = \{\dots, -429, -286, -143, 0, 143, 286, 429, \dots\}$. Selanjutnya sebarang $n \in N$ dengan $n > 0$ sebagai kunci publik. Pada simulasi penelitian ini dipilih $143 \in N$ sebagai kunci publik n sehingga hasil enkripsi dan dekripsi sesuai dengan ASCII *printable characters*.

4. Menentukan fungsi Euler $\phi(N)$ untuk ideal pada ring Dedekind sesuai dengan persamaan (4.2).

   Untuk $M_1 = \langle 11 \rangle$ diperoleh

$$\frac{\mathbb{Z}}{11\mathbb{Z}} = \{0,1,2,3,4,5,6,7,8,9,10\}$$
$$U\left(\frac{\mathbb{Z}}{11\mathbb{Z}}\right) := \left\{a \in \tfrac{\mathbb{Z}}{11\mathbb{Z}} \; \exists \; b \in \tfrac{\mathbb{Z}}{11\mathbb{Z}} \,\middle|\, ab = 1\right\}$$
$$= \{1,2,3,4,5,6,7,8,9,10\}$$
$$\left|U\left(\frac{\mathbb{Z}}{11\mathbb{Z}}\right)\right| = 10$$

   Untuk $M_2 = \langle 13 \rangle$ diperoleh

$$\frac{\mathbb{Z}}{13\mathbb{Z}} = \{0,1,2,3,4,5,6,7,8,9,10,11,12\}$$
$$U\left(\frac{\mathbb{Z}}{13\mathbb{Z}}\right) := \left\{a \in \tfrac{\mathbb{Z}}{13\mathbb{Z}} \; \exists \; b \in \tfrac{\mathbb{Z}}{13\mathbb{Z}} \,\middle|\, ab = 1\right\}$$
$$= \{1,2,3,4,5,6,7,8,9,10,11,12,13\}$$
$$\left|U\left(\frac{\mathbb{Z}}{13\mathbb{Z}}\right)\right| = 12$$

   Selanjutnya dengan persamaan (4.2), diperoleh

$$\begin{aligned}\phi(N) &= |U(R/M_1)|.|U(R/M_2)| \\ &= \left|U\left(\tfrac{\mathbb{Z}}{11\mathbb{Z}}\right)\right|\left|U\left(\tfrac{\mathbb{Z}}{13\mathbb{Z}}\right)\right| \\ &= 10.12 \\ &= 120\end{aligned}$$

Dengan demikian diperoleh nilai $\phi(N)$ yaitu 120

5. Menentukan sebarang bilangan bulat e yang relatif prima terhadap $\phi(N)$. Bilangan bulat ini sebagai kunci publik yang digunakan dalam proses enkripsi. Pada simulasi pembentukan kunci ini dipilih $e = 7$ dengan $\gcd(7, 120) = 1$.
6. Sehingga diperoleh pasangan kunci publik $(143, 7)$ yang selanjutnya dikirimkan kepada pengirim pesan untuk digunakan dalam proses enkripsi pesan.
7. Selanjutnya menghitung kunci privat d dengan persamaan (4.4), sehingga diperoleh

$$\begin{aligned}d &= \tfrac{1+k.\phi(N)}{e} \\ &= \tfrac{1+k.120}{7} \\ &= 103\end{aligned}$$

dengan $k = 1, 2, 3, \ldots \in \mathbb{Z}^+$. Dengan demikian kunci privat d adalah 103.

8. Sehingga penerima pesan memperoleh kunci rahasia $(103, 11, 13)$ yang digunakan untuk proses dekripsi pesan.

Dengan demikian penerima pesan memperoleh pasangan kunci publik dan kunci privat yang digunakan untuk menyandikan pesan dengan algoritma RSA atas ring Dedekind, yaitu kunci publik $(n, e) = (143, 7)$ dan kunci privat

$(d, M_1, M_2) = (103, 11, 13)$. Kunci publik selanjutnya dikirimkan kepada pengirim pesan untuk proses enkripsi, sedangkan kunci privat disimpan oleh penerima pesan untuk proses dekripsi. Dengan demikian pesan tidak dapat didekripsi oleh pihak lain selain penerima yang dituju.

4.2 Proses Enkripsi Pesan dengan Algoritma RSA atas Ring Dedekind

4.2.1 Algoritma Enkripsi RSA atas Ring Dedekind

Proses enkripsi pada algoritma RSA atas ring Dedekind dilakukan sesuai dengan langkah-langkah berikut:

1. Penerima pesan membentuk pasangan kunci, yaitu kunci publik dan kunci privat, kemudian mengirimkan kunci publik kepada pengirim pesan.
2. Pengirim pesan menerima pasangan kunci publik (n, e) yang selanjutnya digunakan untuk proses menyandikan pesan menjadi pesan yang hanya dapat dipahami oleh penerima pesan.
3. Pengirim pesan menentukan pesan m yang dikonversi dalam bentuk angka sesuai dengan ASCII *printable characters* di mana $0 < m < n$. Jika $m \geq n$ maka pesan perlu dibagi menjadi beberapa bagian sehingga m kurang dari n.
4. Selanjutnya melakukan enkripsi pesan dengan persamaan berikut:

$$c = m^e (mod\ n) \tag{4.5}$$

5. Dengan demikian diperoleh pesan yang telah dienkripsi atau cipherteks berupa angka. Cipherteks ini kemudian dikirimkan kepada penerima pesan untuk didekripsi.

4.2.2 Simulasi Enkripsi RSA atas Ring Dedekind

Pada simulasi pembentukan kunci subbab 4.1.2 telah diperoleh pasangan kunci publik $(n, e) = (143, 7)$ dan kunci privat $(d, M_1, M_2) = (103, 11, 13)$, sehingga proses penyandian pesan dapat dilakukan. Berikut merupakan langkah-langkah enkripsi pesan dengan algoritma RSA atas ring Dedekind:

1. Penerima pesan mengirimkan kunci publik $(n, e) = (143, 7)$ kepada pengirim pesan.
2. Pengirim pesan menerima pasangan kunci publik $(n, e) = (143, 7)$ yang digunakan untuk proses enkripsi pesan.
3. Pengirim pesan menentukan pesan yang akan dienkripsi.

   Pada penelitian ini pesan yang digunakan adalah "Kriptografi Kunci Publik" dengan mengabaikan tanda spasi. Plainteks yang digunakan dalam penelitian ini merupakan salah satu jenis kriptografi berdasarkan kunci yang digunakan. Selanjutnya, pesan dikonversi kedalam bentuk angka sesuai dengan ASCII *printable characters* sebagai berikut:

Tabel 4.1 Hasil Konversi Plainteks dalam ASCII

Plainteks	**Indeks**
K	75
r	114
i	105
p	112
t	116
o	111
g	103
r	114

Plainteks	**Indeks**
K	75
u	117
n	110
c	99
i	105
P	80
u	117
b	98

a	97
f	102
i	105

l	108
i	105
k	107

4. Melakukan enkripsi pesan dengan mensubtitusikan indeks plainteks pada Tabel 4.1 dan kunci publik yang telah diperoleh, yaitu $(n, e) = (143, 7)$, dalam persamaan (4.5), dengan demikian diperoleh hasil enkripsi sebagai berikut:

Tabel 4.2 Proses Enkripsi Algoritma RSA atas Ring Dedekind

$\boldsymbol{i}$	**Plainteks**	**Enkripsi** $\boldsymbol{c_i = m_i^7 (mod\ 143)}$	**Cipherteks**
1	75	$75^7 (mod\ 143)$	114
2	114	$114^7 (mod\ 143)$	49
3	105	$105^7 (mod\ 143)$	118
4	112	$112^7 (mod\ 143)$	18
5	116	$116^7 (mod\ 143)$	129
6	111	$111^7 (mod\ 143)$	45
7	103	$103^7 (mod\ 143)$	38
8	114	$114^7 (mod\ 143)$	49
9	97	$97^7 (mod\ 143)$	59
10	102	$102^7 (mod\ 143)$	119
11	105	$105^7 (mod\ 143)$	118
12	75	$75^7 (mod\ 143)$	68
13	117	$117^7 (mod\ 143)$	39
14	110	$110^7 (mod\ 143)$	33
15	99	$99^7 (mod\ 143)$	44
16	105	$105^7 (mod\ 143)$	118
17	80	$80^7 (mod\ 143)$	141
18	117	$117^7 (mod\ 143)$	39
19	98	$98^7 (mod\ 143)$	32

20	108	$108^7 (mod\ 143)$	4
21	105	$105^7 (mod\ 143)$	118
22	107	$107^7 (mod\ 143)$	68

5. Dengan demikian diperoleh pesan yang selanjutnya dikirimkan kepada penerima pesan untuk didekripsi. Cipherteks yang dihasilkan ditunjukkan dalam tabel berikut:

Tabel 4.3. Cipherteks Hasil Enkripsi

C_1	114	C_9	59	C_{17}	141
C_2	49	C_{10}	119	C_{18}	39
C_3	118	C_{11}	118	C_{19}	32
C_4	18	C_{12}	68	C_{20}	4
C_5	129	C_{13}	39	C_{21}	118
C_6	45	C_{14}	33	C_{22}	68
C_7	38	C_{15}	44		
C_8	49	C_{16}	118		

4.3 Proses Dekripsi Pesan dengan Algoritma RSA atas Ring Dedekind

4.3.1 Algoritma Dekripsi RSA atas Ring Dedekind

Proses dekripsi merupakan proses mengembalikan pesan yang telah dienkripsi menjadi pesan awal sesuai dengan kunci yang telah ditentukan. Pada pembentukan kunci, penerima pesan telah memperoleh dua kunci yaitu kunci publik dan kunci privat. Kunci publik akan dikirimkan kepada pengirim pesan sedangkan kunci privat dirahasiakan, sehingga kunci privat hanya diketahui oleh penerima pesan. Hal ini berarti pesan hanya dapat didekripsi oleh pihak yang

memiliki kunci privat yaitu penerima pesan yang dituju. Pada algoritma RSA atas ring Dedekind dilakukan sesuai dengan langkah-langkah berikut:

1. Penerima pesan menerima cipherteks dari pengirim pesan.
2. Penerima pesan melakukan dekripsi cipherteks menggunakan kunci privat yang hanya diketahui oleh penerima pesan dengan persamaan berikut:

   $$m = c^d (mod\ n) \tag{4.6}$$

   Pada Teorema 2.7 telah dibuktikan bahwa persamaan (4.6) dapat mengembalikan cipherteks sesuai dengan plainteks. Sehingga diperoleh hasil dekripsi berupa angka.
3. Selanjutnya mengkonversi hasil dekripsi dalam bentuk karakter sesuai dengan ASCII *printable characters*. Dengan demikian cipherteks yang diterima dapat dikembalikan menjadi plainteks atau pesan awal.

4.3.2 Simulasi Dekripsi RSA atas Ring Dedekind

Pada simulasi enkripsi pesan telah diperoleh cipherteks yang ditunjukkan pada Tabel 4.3. Telah diperoleh pula kunci privat yang digunakan dalam proses dekripsi melalui prose simulasi pembentukan kunci, yaitu $(d, M_1, M_2) = (103, 11, 13)$. Sehingga proses dekripsi pesan dapat dilakukan sesuai dengan algoritma dekripsi sebagai berikut:

1. Penerima pesan menerima cipherteks yang telah ditunjukkan dalam Tabel 4.3.
2. Melakukan dekripsi cipherteks dengan mensubtitusi cipherteks dan kunci privat $(d, M_1, M_2) = (103, 11, 13)$ pada persamaan (4.6) sehingga diperoleh hasil sebagai berikut:

Tabel 4.4 Proses Dekripsi Algoritma RSA atas Ring Dedekind

i	**Cipherteks**	**Dekripsi** $m_i = c_i^{103} (mod\ 143)$	**Plainteks**
1	114	$114^{103} (mod\ 143)$	75
2	49	$49^{103} (mod\ 143)$	114
3	118	$118^{103} (mod\ 143)$	105
4	18	$18^{103} (mod\ 143)$	112
5	129	$129^{103} (mod\ 143)$	116
6	45	$45^{103} (mod\ 143)$	111
7	38	$38^{103} (mod\ 143)$	103
8	49	$49^{103} (mod\ 143)$	114
9	59	$59^{103} (mod\ 143)$	97
10	119	$119^{103} (mod\ 143)$	102
11	118	$118^{103} (mod\ 143)$	105
12	68	$68^{103} (mod\ 143)$	75
13	39	$39^{103} (mod\ 143)$	117
14	33	$33^{103} (mod\ 143)$	110
15	44	$44^{103} (mod\ 143)$	99
16	118	$118^{103} (mod\ 143)$	105
17	141	$141^{103} (mod\ 143)$	80
18	39	$39^{103} (mod\ 143)$	117
19	32	$32^{103} (mod\ 143)$	98
20	4	$4^{103} (mod\ 143)$	108
21	118	$118^{103} (mod\ 143)$	105
22	68	$68^{103} (mod\ 143)$	107

Dengan demikian, diperoleh indeks plainteks hasil dekripsi sebagai berikut:

Tabel 4.5 Hasil Dekripsi Cipherteks

m_1	75	m_9	97	m_{17}	80
m_2	114	m_{10}	102	m_{18}	117
m_3	105	m_{11}	105	m_{19}	98

m_4	112
m_5	116
m_6	111
m_7	103
m_8	114

m_{12}	75
m_{13}	117
m_{14}	110
m_{15}	99
m_{16}	105

m_{20}	108
m_{21}	105
m_{22}	107

3. Mengkonversi hasil dekripsi dalam bentuk karakter sesuai dengan ASCII *printable characters*, sehingga diperoleh hasil dekripsi pesan sebagai berikut:

Tabel 4.6 Hasil Konversi dalam ASCII

Indeks	**Karakter**
75	K
114	r
105	i
112	p
116	t
111	o
103	g
114	r
97	a
102	f
105	i

Indeks	**Karakter**
75	K
117	u
110	n
99	c
105	i
80	P
117	u
98	b
108	l
105	i
107	k

Dengan demikian diperoleh plainteks hasil dekripsi yaitu Kriptografi Kunci Publik.

4.4 Kajian Integrasi Agama

Berdasarkan hasil dan pembahasan diatas, pesan yang dienkripsi algoritma RSA atas ring Dedekind hanya dapat dipecahkan oleh penerima yang dituju yaitu penerima pesan yang memiliki kunci privat. Adapun hasil dekripsi cipherteks menghasilkan pesan yang sesuai dengan plainteks awal tanpa adanya perubahan.

Hal ini menunjukkan bahwa penyandian pesan dengan kriptografi, salah satunya algoritma RSA atas ring Dedekind, merupakan upaya yang dapat dilakukan untuk menjaga kerahasiaan pesan hingga sampai kepada pihak yang berhak menerimanya. Pada subbab 2.2 telah disebutkan bahwa menyampaikan pesan kepada penerima yang berhak tanpa mengubahnya merupakan salah satu bentuk sifat amanah. Tidak hanya menyampaikan pesan saja, namun juga memastikan kerahasiaan tetap terjaga sehingga tidak dapat diketahui dan disalahgunakan oleh pihak yang tidak bertanggung jawab.

Sifat amanah sangat penting bagi kehidupan manusia karena amanah erat kaitannya dengan kepercayaan. Sehingga sebagai seorang mukmin hendaknya menjaga amanah dengan sebaik-baiknya, baik amanat yang berupa benda, perkataan, perbuatan, maupun kepercayaan. Perintah untuk menjaga amanat telah disebutkan dalam beberapa surah dalam Al-Qur'an, bahkan Allah SWT menerangkan bahwa memelihara amanah merupakan salah satu sifat dari seorang mukmin yang beruntung. Hal ini ditunjukkan dalam Al-Qur'an Surah Al-Mu'minun ayat 8 sebagai berikut:

وَالَّذِيْنَ هُمْ لِاَمٰنٰتِهِمْ وَعَهْدِهِمْ رَاعُوْنَ ۙ ﴿٨﴾

Artinya: *"(Sungguh beruntung pula) orang-orang yang memelihara amanat dan janji mereka"*

Demikian pula dalam Al-Qur'an Surah Al-Ma'arij ayat 32 yang berbunyi sebagai berikut:

وَالَّذِيْنَ هُمْ لِاَمٰنٰتِهِمْ وَعَهْدِهِمْ رٰعُوْنَۚ ﴿٣٢﴾

Artinya: *"(Termasuk orang yang selamat dari azab adalah) orang-orang yang memelihara amanat dan janji mereka"*

Sanggup memelihara amanat merupakan salah satu sifat seorang muslim yang membedakan dari orang-orang yang munafik. Sebagaimana sabda Rasulullah

SAW, dalam hadist yang diriwayatkan oleh Imam Bukhari dan Muslim dari Abu Hurairah, terdapat tiga tanda orang munafiq yaitu sebagai berikut:

عَنْ أَبِي هُرَيْرَةَ رَضِيَ الله عَنْهُ قَالَ قَالَ النَّبِيُّ صَلَّى اللهُ عَلَيْهِ وَسَلَّمَ: آيَةُ الْمُنَافِقِ ثَلاَثٌ إِذَا حَدَثَ كَذَبَ وَإِذَا وَعَدَ أَخْلَفَ وَإِذَا ائْتُمِنَ خَانَ

Artinya: *"Tanda-tanda orang munafik itu ada tiga, yaitu: apabila ia berkata, ia berdusta, apabila ia berjanji, ia ingkar (menyalahinya), dan apabila ia diberi amanat, ia berkhianat"*

Namun menjaga amanah bukanlah hal yang mudah untuk dilakukan, sehingga sebagai seorang muslim kita harus berusaha dengan sebaik-baiknya untuk menjaga segala ucapan maupun perbuatan yang diamanatkan kepada kita. Karena apabila amanat tidak lagi terpelihara maka kepercayaan akan hilang, sehingga berakibat ketenangan hidup dalam bermasyarakat tidak dapat lagi dirasakan. Begitu pula dengan menjaga dan menyampaikan amanat yang berupa pesan. Ketika pesan yang sangat penting tidak diamankan dengan baik maka akan dapat disalahgunakan oleh pihak yang tidak bertanggung jawab sehingga merugikan pihak-pihak yang berkomunikasi.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil dan pembahasan di atas, dapat ditarik kesimpulan sebagai berikut:

1. Pada implementasi algoritma RSA atas ring Dedekind, ring Dedekind digunakan dalam proses pembentukan kunci untuk memperoleh kunci privat dan kunci publik. Pasangan bilangan prima pada RSA diganti dengan ideal-ideal maksimal pada ring Dedekind, serta fungsi Euler yang digunakan adalah hasil kali dari kardinalitas grup unit yang ditunjukkan dalam persamaan (4.2). Penggunaan ring Dedekind dalam proses pembentukan kunci menghasilkan pilihan kunci publik yang lebih luas di mana kunci publik yang digunakan merupakan sebarang bilangan positif anggota dari himpunan hasil kali ideal maksimal pada ring Dedekind. Semakin besar nilai kunci publik yang dipilih maka semakin sulit pula pemfaktorannya, sehingga dapat meningkatkan keamanan penyandian pesan.
2. Proses enkripsi pada algoritma RSA atas ring Dedekind dilakukan setelah memperoleh pasangan kunci publik. Proses enkripsi dilakukan dengan mensubtitusikan indeks karakter setiap huruf plainteks dan kunci publik (n, e), di mana n merupakan sebarang bilangan positif anggota dari himpunan hasil kali dua ideal maksimal pada ring Dedekind, ke dalam persamaan enkripsi algoritma RSA atas ring Dedekind yaitu persamaan (4.5). Selanjutnya dilakukan perhitungan sehingga menghasilkan cipherteks.

3. Proses dekripsi pada algoritma RSA atas ring Dedekind dilakukan menggunakan kunci privat yang diperoleh pada proses pembentukan kunci. Proses dekripsi dilakukan dengan mensubtitusikan cipherteks dan kunci privat, yang berupa kunci privat d dan dua ideal maksimal berbeda pada ring Dedekind, ke dalam persamaan dekripsi algoritma RSA atas ring Dedekind yaitu persamaan (4.6). Selanjutnya dilakukan perhitungan sehingga menghasilkan plainteks.

5.2 Saran

Penelitian ini mengimplementasikan algoritma RSA atas ring Dedekind untuk mengamankan pesan teks. Pada penelitian ini, ring Dedekind berperan dalam proses pembentukan kunci, sedangkan untuk proses enkripsi dan dekripsinya menggunakan enkripsi dan dekripsi algoritma RSA. Saran untuk penelitian selanjutnya yaitu melakukan implementasi atau modifikasi dengan metode lain pada algoritma RSA sehingga algoritma yang dihasilkan memiliki tingkat keamanan yang lebih tinggi atau dapat memanfaatkan struktur dari ring Dedekind untuk membentuk algoritma kriptografi lain. Pada simulasi penyandian pesan ring Dedekind yang digunakan adalah ring bilangan bulat, sehingga untuk penelitian selanjutnya disarankan untuk menggunakan ring Dedekind lain.

DAFTAR PUSTAKA

Abdul Baqi, M. F. (2017). *Shahih Bukhari Muslim*. Lontar Mediatama.

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi* (1st ed.). Perpustakaan Badan Pengusahaan Batam.

El-Kassar, A. N., Haraty, R. A., & Awad, Y. (2005). Modified RSA in the Domains of Gaussian Integers and Polunomial Over Finite Fields. *Proceedings of the ISCA 18th International Conference on Computer Applications in Industry and Engineering*.

Ginting, D. B. (2010). Peranan Aritmetika Modulo dan Bilangan Prima pada Algoritma Kriptografi RSA (Rivest-Shamir-Adleman). *Media Informatika*, *9*(2).

Hodge, J. K., Schlicker, S., & Sundstrom, T. (2013). *Abstract Algebra: An Inquiry-Based Approach* (A. Boggess (ed.)). CRC Press.

Hungerford, T. W. (2000). *Algebra* (S. Axler, F. W. Gehring, & K. A. Ribet (eds.)). Springer-Verlag New York, Inc.

Ibnu Katsir, A.-I. A. F. I. (2008). *Tafsir Ibnu Katsir*. Sinar Baru Algensindo.

Jankowska, M., & Matysiak, L. (2022). A structure of Dedekind in the cryptosystem. *SCIREA Journal of Mathematics*, *7*(1), 30–37. https://doi.org/10.54647/mathematics11310

Kemenag. (2019). *Tafsir Kemenag*. https://kemenag.go.id

Kraft, J. S., & Washington, L. C. (2016). *An Introduction to Number Theory with Cryptography*. CRC Press.

Lajnah Pentashihan Mushaf Al-Qur'an. (2018). *Al-Qur'an dan Terjemahnya*. Tiga Serangkai Pustaka Mandiri.

Linuhung, N. (2018). Teori Bilangan. In *Paper Knowledge . Toward a Media History of Documents*. Universitas Muhammadiyah Metro.

Menezes, A. J., Oorschot, P. C. van, & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.

Mukhtar, H. (2018). *Kriptografi untuk Keamanan Data* (Ed. 1). Deepublish.

Munawwir, A. W. (1984). *Kamus Al-Munawwir Arab-Indonesia Terlengkap*. Pustaka Progressif.

Munir, R. (2006). Kriptografi. *Informatika, Bandung*.

Munir, R. (2016). *Matematika Diskrit* (Revisi Kee). Informatika Bandung.

Munir, R. (2018). Pengantar Kriptografi. *Informatika, Bandung*, 52.

Persulessy, E. R., & Dahoklory, N. (2015). Karakterisasi Daerah Dedekind. *BAREKENG: Jurnal Ilmu Matematika Dan Terapan*, *9*(1), 1–10.

https://doi.org/10.30598/barekengvol9iss1pp1-10

Petukhova, K. A., & Tronin, S. N. (2016). *RSA Cryptosystem for Dedekind Rings*. *37*(3), 284–287. https://doi.org/10.1134/S1995080216030197

Wahyuni, S., Wijayanti, I. E., Yuwaningsih, D. A., & Hartanto, A. D. (2017). *Teori Ring dan Modul*. Gadjah Mada University Press.

Wijayanti, I. E. (2022). Contributions of Algebra in Cryptography Abstraction of RSA. *International Conference on Green Technology Faculty of Science and Technology*, 26–27.

LAMPIRAN

Lampiran 1. Tabel ASCII 0-126

Indeks	Simbol	Keterangan
000	NULL	*NULL character*
001	SOH	*Start of Heading*
002	STX	*Start of Text*
003	ETX	*End of Text*
004	EOT	*End of Transmission*
005	ENX	*Enquiry*
006	ACK	*Acknowledgement*
007	BEL	*Bell*
008	BS	*Backspace*
009	HT	*Horizontal Tab*
010	LF	*Line Feed*
011	VT	*Vertical Tab*
012	FF	*Form Feed*
013	CR	*Carriage Return*
014	SO	*Shift Out*
015	SI	*Shift In*
016	DLE	*Data Link Escape*
017	DC1	*Device Control 1*
018	DC2	*Device Control 2*
019	DC3	*Device Control 3*
020	DC4	*Device Control 4*
021	NAK	*Negative Acknowledgement*
022	SYN	*Synchronous Idle*
023	ETB	*End of Trans. Block*

024	CAN	*Cancel*
025	EM	*End of Medium*
026	SUB	*Subtitute*
027	ESC	*Escape*
028	FS	*File Separator*
029	GS	*Group Separator*
030	RS	*Record Separator*
031	US	*Unit Separator*
032	Space	*Space*
033	!	*Exclamation Mark*
034	"	*Quotation Mark*
035	#	*Number Sign*
036	$	*Dollar Sign*
037	%	*Percent Sign*
038	&	*Ampersand*
039	'	*Apostrophe*
040	(	*Round Brackets*
041	)	*Round Brackets*
042	*	*Asterisk*
043	+	*Plus Sign*
044	,	*Comma*
045	-	*Hyphen*
046	.	*Dot, Full Stop*
047	/	*Slash*
048	0	*Number Zero*
049	1	*Number One*
050	2	*Number Two*

051	3	*Number Three*
052	4	*Number Four*
053	5	*Number Five*
054	6	*Number Six*
055	7	*Number Seven*
056	8	*Number Eight*
057	9	*Number Nine*
058	:	*Colon*
059	;	*Semicolon*
060	<	*Less-Than Sign*
061	=	*Equals Sign*
062	>	*Greater-Than Sign*
063	?	*Question Mark*
064	@	*At Sign*
065	A	*Capital Letter A*
066	B	*Capital Letter B*
067	C	*Capital Letter C*
068	D	*Capital Letter D*
069	E	*Capital Letter E*
070	F	*Capital Letter F*
071	G	*Capital Letter G*
072	H	*Capital Letter H*
073	I	*Capital Letter I*
074	J	*Capital Letter J*
075	K	*Capital Letter K*
076	L	*Capital Letter L*
077	M	*Capital Letter M*

078	N	*Capital Letter N*
079	O	*Capital Letter O*
080	P	*Capital Letter P*
081	Q	*Capital Letter Q*
082	R	*Capital Letter R*
083	S	*Capital Letter S*
084	T	*Capital Letter T*
085	U	*Capital Letter U*
086	V	*Capital Letter V*
087	W	*Capital Letter W*
088	X	*Capital Letter X*
089	Y	*Capital Letter Y*
090	Z	*Capital Letter Z*
091	[	*Square Brackets*
092	\	*Backslash*
093	]	*Square Brackets*
094	^	*Circumflex Accent*
095	_	*Underscore*
096	`	*Grave Accent*
097	a	*Lowercase Letter A*
098	b	*Lowercase Letter B*
099	c	*Lowercase Letter C*
100	d	*Lowercase Letter D*
101	e	*Lowercase Letter E*
102	f	*Lowercase Letter F*
103	g	*Lowercase Letter G*
104	h	*Lowercase Letter H*

105	i	*Lowercase Letter I*
106	j	*Lowercase Letter J*
107	k	*Lowercase Letter K*
108	l	*Lowercase Letter L*
109	m	*Lowercase Letter M*
110	n	*Lowercase Letter N*
111	o	*Lowercase Letter O*
112	p	*Lowercase Letter P*
113	q	*Lowercase Letter Q*
114	r	*Lowercase Letter R*
115	s	*Lowercase Letter S*
116	t	*Lowercase Letter T*
117	u	*Lowercase Letter U*
118	v	*Lowercase Letter V*
119	w	*Lowercase Letter W*
120	x	*Lowercase Letter X*
121	y	*Lowercase Letter Y*
122	z	*Lowercase Letter Z*
123	{	*Curly Brackets*
124	|	*Vertical Bar*
125	}	*Curly Brackets*
126	~	*Tilde*
127	DEL	*Delete*

RIWAYAT HIDUP

Zakiyya Dzul Ladunniyyah, lahir di Kabupaten Tulungagung pada tanggal 25 November 2000, biasa dipanggil Zakiyya. Merupakan putri pertama dari bapak Ahmad Sumari dan ibu Suharti serta kakak dari dua adik yang bernama Shofiyya Quthbil Ma'rifah dan Balqis Tajalliyyal Haq. Penulis bertempat tinggal di Dusun Tambak, Desa Pelem, Kecamatan Campurdarat, Kabupaten Tulungagung, Jawa Timur. Pendidikan pertama penulis ditempuh di TK Plus Al-Ikhlas Pucungkidul dan lulus pada tahun 2007. Kemudian, melanjutkan pendidikan dasar di SDN 2 Pelem dan lulus pada tahun 2013. Penulis kemudian melanjutkan pendidikan sekolah menengah pertama di MTsN 1 Tulungagung dan lulus pada tahun 2016. Setelah itu, melanjutkan pendidikan menengah atas di MAN 2 Tulungagung dan lulus pada tahun 2019. Selanjutnya pada tahun 2019, penulis memulai jenjang pendidikan perguruan tinggi di Universitas Islam Negeri Maulana Malik Ibrahim Malang dengan mengambil Program Studi Matematika, 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 : Zakiyya Dzul Ladunniyyah
NIM : 19610048
Fakultas/Program Studi : Sains dan Teknologi/Matematika
Judul Skripsi : Implementasi Algoritma *Rivest Shamir Adleman* atas Ring Dedekind untuk Mengamankan Pesan Teks
Pembimbing I : Muhammad Khudzaifah, M.Si.
Pembimbing II : Erna Herawati, M.Pd.

No	Tanggal	Hal	Tanda Tangan
1.	11 Januari 2023	Konsultasi BAB I	1.
2.	14 Maret 2023	Konsultasi Revisi BAB I	2.
3.	15 Maret 2023	Konsultasi BAB II dan BAB III	3.
4.	28 Maret 2023	Konsultasi Revisi BAB II dan BAB III	4.
5.	29 Maret 2023	Konsultasi Kajian Agama BAB I dan BAB II	5.
6.	11 April 2023	Konsultasi Revisi Kajian Agama BAB I dan BAB II	6.
7.	16 Mei 2023	ACC Seminar Proposal	7.
8.	13 September 2023	Konsultasi BAB IV	8.
9.	19 September 2023	Konsultasi Revisi BAB IV	9.
10.	21 September 2023	Konsultasi Kajian Agama BAB IV	10.
11.	22 September 2023	Konsultasi Revisi Kajian Agama BAB IV	11.
12.	27 September 2023	Konsultasi Revisi BAB IV dan Konsultasi BAB V	12.
13.	10 Oktober 2023	ACC Seminar Hasil	13.
14.	31 Oktober 2023	Konsultasi Revisi Seminar Hasil	14.
15.	2 November 2023	Konsultasi Revisi Seminar Hasil	15.
16.	3 November 2023	Konsultasi Kajian Agama BAB IV	16.

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

17.	16 November 2023	ACC Matriks Revisi Seminar Hasil	17.
18.	29 November 2023	ACC Sidang Skripsi	18.
19.	13 Desember 2023	ACC Keseluruhan	19.

Malang, 13 Desember 2023
Mengetahui,
Ketua Program Studi Matematika

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