Jurnal Riset Mahasiswa Matematika
Volume 3(4) (2024), Pages 157-165
p-ISSN: 2808-1552; e-ISSN: 2808-4926

Implementasi Algoritma Rivest Shamir Adleman atas Ring Dedekind

Zakiyya Dzul Ladunniyyah*, Muhammad Khudzaifah, Erna Herawati

Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang, Indonesia

zakiyyadl@gmail.com*, khudzaifah@uin-malang.ac.id, faridatul_mahya@uin-malang.ac.id

Abstrak

Masalah keamanan dan kerahasiaan data atau pesan merupakan hal yang sangat penting sehingga diperlukan upaya untuk menjaga keamanan dan kerahasiaan pesan, salah satunya dengan Kriptografi. Penelitian ini bertujuan untuk mengetahui 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. Tahapan penelitian yang dilakukan yaitu melakukan pembentukan kunci pada algoritma RSA atas ring Dedekind, selanjutnya mengonstruksi algoritma enkripsi dan dekripsi untuk mengamankan pesan dengan RSA atas ring Dedekind. Dari penelitian ini diperoleh hasil berupa algoritma penyandian pesan RSA yang sesuai dengan ring Dedekind di mana ring Dedekind digunakan pada proses pembentukan kunci. Selanjutnya proses enkripsi dan dekripsi dilakukan dengan algoritma RSA. 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 anggota dari himpunan hasil kali ideal maksimal pada ring Dedekind.

Kata kunci: algoritma RSA; kriptografi; ring Dedekind

Abstract

The issue of security and confidentiality of data or messages is very important so efforts are needed to maintain the security and confidentiality of messages, one of which is with cryptography. This study aims to determine 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. 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. From this research, results were obtained in the form of an RSA message encoding algorithm in accordance with the Dedekind ring where the Dedekind ring was used in the key formation process. Furthermore, the encryption and decryption process is carried out with the RSA algorithm. 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 member number of the set of maximal ideal products on the Dedekind ring.

Keywords: RSA algorithm; cryptography; Dedekind ring

PENDAHULUAN

Perkembangan teknologi di bidang informasi dan komunikasi memberikan banyak manfaat salah satunya adalah mempermudah pertukaran informasi, baik yang bersifat umum maupun rahasia. Namun, kemajuan teknologi juga dapat mempermudah aktivitas kejahatan yang mengganggu privasi seseorang. Misalnya penyadapan atau pencurian data-data pribadi untuk disalahgunakan sehingga merugikan korban. Hal ini menunjukkan bahwa masalah keamanan dan kerahasiaan pesan atau data merupakan hal yang penting sehingga diperlukan upaya untuk menjaga keamanan pesan atau data, salah satunya dengan kriptografi [1]. Kriptografi merupakan

Submitted: 22 Januari 2023 Reviewed: 16 September 2023 Accepted: 18 Maret 2024
Doi: http://dx.doi.org/10.18860/jrmm.v3i4.25407

ilmu sekaligus seni untuk menjaga keamanan pesan dengan menyandikan pesan tersebut menjadi pesan acak yang tidak bermakna [2]-[3]. Kriptografi berkaitan dengan aspek keamanan informasi seperti tingkat kenyamanan, integritas data, autentikasi data, serta identifikasi keaslian data [4]. Tujuan dari kriptografi bukan untuk menyembunyikan pesan, melainkan menyembunyikan makna dari suatu pesan sehingga pesan hanya dapat dipahami penerima yang dituju [5].

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. Algoritma *Rivest Shamir Adleman* (RSA) merupakan salah satu algoritma kriptografi kunci publik, yaitu algoritma yang menggunakan dua kunci berbeda pada proses enkripsi dan dekripsinya [6]-[7]. Algoritma RSA memiliki pengaruh yang besar dalam perkembangan teori bilangan, di mana algoritma ini menunjukkan bahwa cukup mudah mengalikan dua bilangan prima besar namun sulit untuk memfaktorkan bilangan secara efisien [8]. Sehingga topik mengenai faktorisasi dan menemukan bilangan prima menjadi popular dan terus mengalami kemajuan, bahkan batas kemampuan teknologi dalam faktorisasi bilangan saat ini telah lebih dari 230 digit bilangan [9]. Hal ini menunjukkan bahwa terdapat kemungkinan segera ditemukannya algoritma yang efisien untuk faktorisasi sehingga beberapa algoritma kriptografi, seperti RSA, terancam dapat dipecahkan dengan mudah. Dengan demikian diperlukan adanya modifikasi untuk meningkatkan keamanan dari algoritma tersebut [10].

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 primanya [11]. Suatu ring disebut Dedekind jika dan hanya jika tertutup secara integral, berupa ring *noetherian*, dan setiap ideal tak nolnya adalah ideal maksimal [12].

Penelitian mengenai modifikasi algoritma RSA untuk meningkatkan keamanan RSA telah beberapa kali dilakukan. Khudzaifah, Ma'rifah dan Fahmi melakukan penelitian mengenai implementasi algoritma *Rubik's Cube* dan RSA pada keamanan digital. Berdasarkan penelitian ini, penggunaan algoritma *Rubik's Cube* dan RSA dalam enkripsi dan dekripsi didapatkan nilai kunci maksimum dan semakin besar nilai kunci maka diperlukan waktu yang lebih banyak untuk prosesnya[13]. Selanjutnya implementasi algoritma kriptografi atas ring Dedekind juga telah beberapa kali telah dilakukan, baik dengan memodifikasi proses pembentukan kunci maupun proses enkripsi dan dekripsinya agar sesuai dengan ring Dedekind yang digunakan. Pada penelitian yang dilakukan oleh El-Kassar, Haraty, dan Awad menghasilkan modifikasi algoritma RSA yang sesuai dengan beberapa ring Dedekind, yaitu ring Gaussian dan ring Polinomial [14]. Namun dalam penelitian ini, setiap algoritma yang dihasilkan hanya berlaku untuk salah satu jenis ring Dedekind saja. Selanjutnya, pada penelitian Jankowska dan Matysiak, peneliti membentuk beberapa algoritma kriptografi secara umum berdasarkan struktur dari ring Dedekind [15].

Berdasarkan penelitian yang telah dikemukakan sebelumnya, dalam penelitian ini akan dilakukan implementasi algoritma RSA atas ring Dedekind sehingga dapat meningkatkan keamanan penyandian pesan. 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 dilakukan proses enkripsi dan dekripsi untuk menyandikan pesan teks dengan algoritma RSA.

METODE

Langkah-langkah Penelitian

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.

2. Mengonstruksi algoritma enkripsi pesan 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.
3. Mengonstruksi algoritma dekripsi pesan 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.

HASIL DAN PEMBAHASAN

Algoritma Pembentukan Kunci RSA atas Ring Dedekind

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 algoritma RSA atas ring Dedekind, ring Dedekind akan digunakan dalam proses pembentukan kunci sehingga diperoleh kunci publik dan kunci privat yang akan digunakan. 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 N yang merupakan hasil kali dari dua ideal maksimal dari ring Dedekind D yang telah ditentukan, atau dapat dituliskan sebagai berikut:
   $$N = M_1.M_2 \quad (1)$$
   Sehingga diperoleh himpunan N yang merupakan himpunan bilangan hasil kali dari dua ideal maksimal. Selanjutnya dipilih sebarang $n \in N$ dengan $n > 0$ dijadikan sebagai kunci publik n. Sehingga terdapat beberapa pilihan bilangan yang dapat dijadikan sebagai kunci publik n, semakin besar nilai n yang dipilih maka semakin sulit pula pemfaktorannya.
4. Menentukan fungsi euler $\phi(N)$ untuk ideal pada ring Dedekind yang berupa hasil kali dari kardinalitas grup unit [10].
   $$\phi(N) = |U(R/M_1)|.|U(R/M_2)| \quad (2)$$
5. Menentukan sebarang bilangan bulat e sebagai kunci publik yang relatif prima terhadap $\phi(N)$ yaitu dengan $\gcd(e, \phi(N)) = 1$.
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
   $$ed \equiv 1(mod\ \phi(N)) \quad (3)$$
   Karena $ed \equiv 1(mod\ \phi(N))$ ekuivalen dengan $ed = 1 + k.\varphi(N)$ maka d dapat dihitung dengan persamaan berikut:
   $$d = \frac{1 + k.\phi(N)}{e} \quad (4)$$
   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.

Simulasi Pembentukan Kunci Algoritma RSA atas Ring Dedekind

1. Menentukan ring Dedekind D yang yang telah memenuhi syarat ring Dedekind yaitu merupakan ring *Noether,* tertutup secara integral, dan setiap ideal prima tak nol dari $\mathbb{Z}$ merupakan ideal maksimal [15].
2. Menentukan dua ideal maksimal yang berbeda yaitu M_1 dan M_2 dari ring $\mathbb{Z}$. Dipilih $M_1 = \langle 11\rangle$dan $M_2 = \langle 13\rangle$.
3. Menghitung N dengan persamaan (1), sehingga diperoleh sebagai berikut:
$$\begin{aligned} N &= M_1.M_2 \\ &= 11\mathbb{Z}.13\mathbb{Z} \\ &= 143\mathbb{Z} \end{aligned}$$
Selanjutnya dipilih $143 \in N$ sebagai kunci publik n.
4. Menentukan fungsi euler $\phi(N)$ untuk ideal pada ring Dedekind sesuai dengan persamaan (2), yaitu hasil kali dari kardinalitas grup unit atau himpunan elemen yang memiliki invers terhadap perkalian [16].
Untuk $M_1 = \langle 11\rangle$ diperoleh
$$\mathbb{Z}/11\mathbb{Z} = \{0,1,2,3,4,5,6,7,8,9,10\}$$
$$U(\mathbb{Z}/11\mathbb{Z}) = \{1,2,3,4,5,6,7,8,9,10\}$$
$$|U(\mathbb{Z}/11\mathbb{Z})| = 10$$
Untuk $M_2 = \langle 13\rangle$ diperoleh
$$\mathbb{Z}/13\mathbb{Z} = \{0,1,2,3,4,5,6,7,8,9,10,11,12\}$$
$$U(\mathbb{Z}/13\mathbb{Z}) = \{1,2,3,4,5,6,7,8,9,10,11,12\}$$
$$|U(\mathbb{Z}/13\mathbb{Z})| = 12$$
Selanjutnya dengan persamaan (2), diperoleh
$$\begin{aligned} \phi(N) &= |U(R/M_1)|.|U(R/M_2)| \\ &= |U(\mathbb{Z}/11\mathbb{Z})||U(\mathbb{Z}/13\mathbb{Z})| \\ &= 120 \end{aligned}$$
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), sehingga diperoleh
$$\begin{aligned} d &= \frac{1+k.120}{7} \\ &= 103 \end{aligned}$$
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 $(d, M_1, M_2) = (103, 11, 13)$.

Enkripsi dengan Algoritma RSA atas Ring Dedekind

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 $0 \leq m < n$. Jika $m \geq n$ maka pesan perlu dibagi menjadi beberapa bagian sehingga m kurang dari n.
4. Selanjutnya melakukan enkripsi pesan dengan persamaan berikut:
$$c = m^e (mod\ n) \quad (5)$$
5. Dengan demikian diperoleh pesan yang telah dienkripsi atau cipherteks berupa angka. Cipherteks ini kemudian dikirimkan kepada penerima pesan untuk didekripsi.

Simulasi Enkripsi 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. Selanjutnya, pesan dikonversi kedalam bentuk angka sesuai dengan ASCII *printable characters* sebagai berikut:

Tabel 1. Hasil Konversi Plainteks dalam ASCII

Plainteks	Indeks	Plainteks	Indeks
K	75	K	75
r	114	u	117
i	105	n	110
p	112	c	99
t	116	i	105
o	111	P	80
g	103	u	117
r	114	b	98
a	97	l	108
f	102	i	105
i	105	k	107

4. Melakukan enkripsi pesan dengan mensubtitusikan indeks plainteks dan kunci publik yang telah diperoleh, yaitu $(n, e) = (143, 7)$, dalam persamaan (5), sehingga diperoleh hasil sebagai berikut:

Tabel 2. Proses Enkripsi Algoritma RSA atas Ring Dedekind

i	Plainteks	Enkripsi $c_i = m_i^7 (mod\ 143)$	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

i	**Plainteks**	**Enkripsi** $c_i = m_i^7 (mod\ 143)$	**Cipherteks**

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

Tabel 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		

Dekripsi dengan Algoritma RSA atas Ring Dedekind

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:

$$m = c^d (mod\ n) \quad (6)$$

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.

Simulasi Dekripsi dengan Algoritma RSA atas Ring Dedekind

1. Penerima pesan menerima cipherteks yang telah ditunjukkan dalam Tabel 3.
2. Melakukan dekripsi cipherteks menggunakan kunci privat $(d, M_1, M_2) = (103, 11, 13)$ dengan persamaan (6) sebagai berikut:

Tabel 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
$\boldsymbol{i}$	**Cipherteks**	**Dekripsi** $\boldsymbol{m_i = c_i^{103}(mod\ 143)}$	**Plainteks**
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

Sehingga diperoleh hasil dekripsi sebagai berikut:

Tabel 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_{12}	75	m_{20}	108
m_5	116	m_{13}	117	m_{21}	105
m_6	111	m_{14}	110	m_{22}	107
m_7	103	m_{15}	99		
m_8	114	m_{16}	105		

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

Tabel 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.

KESIMPULAN

Pada implementasi algoritma RSA atas ring Dedekind, ring Dedekind digunakan dalam proses pembentukan kunci untuk memperoleh kunci privat dan kunci publik. Kunci publik n berupa sebarang bilangan anggota dari himpunan N yang merupakan hasil kali dua ideal maksimal pada ring Dedekind yang digunakan. Selanjutnya fungsi euler yang digunakan adalah fungsi euler untuk ring Dedekind yang ditunjukkan dalam persamaan (2). Selanjutnya, proses penyandian dilakukan dengan persamaan enkripsi dan dekripsi RSA. Penggunaan ring Dedekind dalam algoritma ini dapat menghasilkan kunci publik yang lebih luas daripada algoritma RSA, sehingga dapat meningkatkan keamanan dalam penyandian pesan.

DAFTAR PUSTAKA

[1] D. Ariyus, *Pengantar Ilmu Kriptografi*, 1st ed. Yogyakarta: Perpustakaan Badan Pengusahaan Batam, 2008.

[2] R. Munir, *Matematika Diskrit*, Revisi Kee. Bandung: Informatika Bandung, 2016.

[3] H. Mukhtar, *Kriptografi untuk Keamanan Data*, Ed. 1. Yogyakarta: Deepublish, 2018.

[4] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. United States of America: CRC Press, 1996.

[5] R. Munir, "Kriptografi," *Inform. Bandung*, 2006.

[6] R. Munir, "Pengantar Kriptografi," *Inform. Bandung*, p. 52, 2018.

[7] R. Munir, "Algoritma RSA," 2020.

[8] J. K. Hodge, S. Schlicker, and T. Sundstrom, *Abstract Algebra: An Inquiry-Based Approach*. Michigan, USA: CRC Press, 2013.

[9] J. S. Kraft and L. C. Washington, *An Introduction to Number Theory with Cryptography*. Maryland, USA: CRC Press, 2016.

[10] K. A. Petukhova and S. N. Tronin, "RSA Cryptosystem for Dedekind Rings," vol. 37, no. 3, pp. 284–287, 2016, doi: 10.1134/S1995080216030197.

[11] E. R. Persulessy and N. Dahoklory, "Karakterisasi Daerah Dedekind," *BAREKENG J. Ilmu Mat. dan Terap.*, vol. 9, no. 1, pp. 1–10, 2015, doi: 10.30598/barekengvol9iss1pp1-10.

[12] I. E. Wijayanti, "Contributions of Algebra in Cryptography Abstraction of RSA," *Int. Conf. Green Technol. Fac. Sci. Technol.*, pp. 26–27, 2022.

[13] M. Khudzaifah, S. H. Ma'rifah, and H. Fahmi, *Implementation of Rubik's Cube Algorithm and Rivest-Shamir-Adleman (RSA) Algorithm on Iris Digital Image Security*, vol. 2. Atlantis Press International BV, 2023. doi: 10.2991/978-94-6463-148-7_31.

[14] A. N. El-Kassar, R. A. Haraty, and Y. Awad, "Modified RSA in the Domains of Gaussian Integers and Polunomial Over Finite Fields," *Proc. ISCA 18th Int. Conf. Comput. Appl. Ind. Eng.*, 2005.

[15] M. Jankowska and L. Matysiak, "A structure of Dedekind in the cryptosystem," *SCIREA J. Math.*, vol. 7, no. 1, pp. 30–37, 2022, doi: 10.54647/mathematics11310.

[16] S. Wahyuni, I. E. Wijayanti, D. A. Yuwaningsih, and A. D. Hartanto, *Teori Ring dan Modul*. Yogyakarta: Gadjah Mada University Press, 2017.