Jurnal Riset Mahasiswa Matematika
Volume 4 (6) (2025), Pages 301-309
p-ISSN: 2808-1552; e-ISSN: 2808-4926

Pemanfaatan Persamaan Diophantine Linear dalam Membangkitkan Kunci Privat pada Algoritma RSA

Tahang Purwandi* and Syamsyida Rozi

Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Jambi, Indonesia

Abstrak

Algoritma RSA adalah salah satu algoritma kriptografi kunci publik yang paling banyak digunakan karena keamanannya didasarkan pada sulitnya memfaktorkan bilangan bulat besar. Salah satu tahapan penting dalam algoritma RSA adalah pembangkitan kunci privat, yang secara matematis melibatkan penyelesaian persamaan bilangan bulat. Penelitian ini bertujuan untuk menjelaskan secara formal bahwa proses tersebut dapat dirumuskan sebagai persoalan persamaan Diophantine linear. Metode yang digunakan meliputi transformasi persamaan kongruensi menjadi bentuk persamaan linear dua variabel dan penyelesaiannya menggunakan algoritma Euclid yang diperluas. Studi kasus dilakukan dengan memilih dua bilangan prima besar dan nilai kunci publik tertentu. Hasilnya menunjukkan bahwa nilai kunci privat sebesar 1197031 dapat diperoleh dari penyelesaian persamaan Diophantine dan berhasil digunakan untuk mendekripsi pesan menjadi teks semula secara tepat. Penelitian ini menunjukkan bahwa struktur matematis dari algoritma RSA dapat dijelaskan sepenuhnya melalui pendekatan teori bilangan, sehingga memperkuat pemahaman konseptual terhadap algoritma tersebut.

Kata Kunci: Algoritma Euclid; Algoritma RSA; Kriptografi; Persamaan Diophantine Linear; Teori Bilangan

Abstract

The RSA algorithm is one of the most widely used public-key cryptographic algorithms due to its security, which is based on the difficulty of factoring large integers. One of the crucial steps in this algorithm is the generation of the private key, which mathematically involves solving an integer equation. This study aims to formally demonstrate that this process can be formulated as a linear Diophantine equation problem. The method involves transforming a congruence equation into a two-variable linear equation and solving it using the extended Euclidean algorithm. A case study is conducted by selecting two large prime numbers and a specific public key value. The results show that a private key value of 1197031 can be obtained from the solution of the Diophantine equation and successfully used to decrypt the message back into its original text. These findings indicate that the mathematical structure of the RSA algorithm can be fully explained through an elementary number theory approach, thereby enhancing conceptual understanding of the algorithm.

Keywords: Cryptography; Euclidean algorithm; Linear Diophantine Equation; Number Theory; RSA algorithm

*Corresponding author. E-mail: tahangpurwanditahang@gmail.com

Submitted: 22 Juni 2025 Reviewed: 14 Juli 2025 Accepted: 7 Agustus 2025
DOI: https://doi.org/10.18860/jrmm.v4i6.34656

1 Pendahuluan

Perkembangan teknologi dan informasi di era modern sangatlah pesat, sehingga menuntut adanya sistem keamanan digital yang kuat dan andal [1]. Dalam konteks ini, kriptografi memiliki peran penting sebagai basis utama dalam menjaga kerahasiaan, integritas, dan autentikasi data [2]. Beberapa algoritma kriptografi kunci publik yang paling banyak digunakan hingga saat ini adalah algoritma RSA, yang dasar keamanannya terdapat pada sukarnya memfaktorkan bilangan bulat besar menjadi faktor-faktor prima [3].

Algoritma RSA tidak hanya dikenal karena kekuatan keamanannya, tetapi juga karena keterkaitannya yang erat dengan struktur-struktur matematika klasik, khususnya dalam teori bilangan. Salah satu tahap penting dalam algoritma RSA adalah pembangkitan kunci privatnya, yang secara teoritis melibatkan penyelesaian persamaan bilangan bulat. Masalah ini termasuk dalam ranah persamaan Diophantine linear, yaitu persamaan yang penyelesaiannya berada pada himpunan bilangan bulat untuk koefisien yang juga merupakan bilangan bulat [4].

Persamaan Diophantine linear merupakan salah satu tema mendasar dalam teori bilangan dan banyak diaplikasikan dalam bidang kriptografi [5]. Sejumlah penelitian telah menunjukkan peran penting persamaan ini dalam pengembangan sistem kriptografi modern, termasuk dalam pembentukan sistem kunci algoritma RSA yang aman dan efisien [6]. Selain itu, penyelesaian persamaan Diophantine linear umumnya dilakukan menggunakan algoritma Euclid atau algoritma Euclid yang diperluas, yang memungkinkan pencarian solusi bilangan bulat lebih efisien [7].

Meskipun pemanfaatan persamaan Diophantine linear dalam algoritma RSA telah menjadi bagian dari penjelasan standar dalam teori kriptografi, masih sedikit pengamatan secara eksplisit dan formal menjelaskan bagaimana struktur persamaan Diophantine secara matematis berperan dalam membangkitkan kunci privat pada algoritma RSA. Penelitian ini bertujuan mengisi kesenjangan tersebut dengan menyajikan kajian teoritis yang memformulasikan secara eksplisit penyelesaian persamaan Diophantine linear dalam konteks algoritma RSA.

Penelitian ini bertujuan untuk menjelaskan secara formal bagaimana persamaan Diophantine linear digunakan dalam proses pembangkitan kunci privat pada algoritma RSA, serta mengekspos bahwa struktur matematis dari algoritma RSA dapat dijelaskan secara menyeluruh melalui pendekatan teori bilangan elementer. Kajian ini diharapkan dapat memberikan kontribusi terhadap pemahaman konsep dasar dari algoritma RSA, serta menekankan pentingnya basis matematis dalam pengembangan suatu algoritma kriptografi.

Kontribusi orisinal dari penelitian ini terdapat pada penekanan bagian formalisasi matematika dari pembangkitan kunci algoritma RSA, yang secara eksplisit diformulasikan sebagai persoalan penyelesaian persamaan Diophantine linear.

2 Konsep Dasar

Untuk menjabarkan bagaimana persamaan Diophantine linear digunakan dalam pembangkitan kunci privat dalam algoritma RSA, bagian ini akan mengulas konsep-konsep dasar yang relevan. Kajian dimulai dari prinsip kriptografi kunci publik, mekanisme kerja algoritma RSA, hingga teknik penyelesaian persamaan bilangan bulat. Pemahaman terhadap konsep-konsep ini sangat penting sebagai landasan untuk memahami bagian formal dalam hasil utama.

2.1 Algoritma RSA

Algoritma RSA merupakan algoritma kriptografi kunci publik yang diciptakan oleh tiga orang peneliti asal *Massachusetts Institute of Technology* pada tahun 1976 yaitu Ron Rivest, Adi Shamir dan Leonard Adleman [8].
Proses dasar algoritma RSA [9]:

1. Memilih dua buah bilangan prima yang berbeda p dan q.

2. Menghitung $n = p \cdot q$.
3. Menghitung fungsi *totient* Euler: $\phi(n) = (p-1)(q-1)$.
4. Memilih bilangan bulat e yang berada dalam interval tutup $(1,\ \phi(n))$, dengan FPB$(e,\ \phi(n)) = 1$.
5. Menentukan d sebagai invers modulo dari e terhadap $\phi(n)$, sehingga $e \cdot d \equiv 1\ (mod\ \phi(n))$.
6. kunci publik $= (n, e)$ dan kunci privat $= (n, d)$.
7. Fungsi enkripsi $c = E_e(m) = m^e\ (mod\ n)$.
8. Fungsi Dekripsi $m = D_d(c) = c^d\ (mod\ n)$.

2.2 Formulasi Algoritma RSA

Algoritma RSA merupakan algoritma kriptografi yang berlandaskan pada teorema Euler yang dinyatakan bahwa [10]:

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

dengan syarat:

1. a harus relatif prima terhadap n.
2. Fungsi $\phi(n)$ adalah fungsi *totient* Euler yang menentukan berapa banyak bilangan bulat positif yang lebih kecil dari n dan relatif prima terhadap n. Fungsi ini didefinisikan sebagai berikut:
$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})...(1 - \frac{1}{p_r})$$
dengan $p_1, p_2, ..., p_r$ adalah faktor-faktor prima dari n.

Berdasarkan sifat kekongruenan, jika $a \equiv b\ (mod\ n)$, maka $a^k = b^k\ (mod\ n)$ untuk setiap bilangan bulat positif k. Maka Persamaan (1) dapat ditulis ulang sebagai:

$$a^{k \cdot \phi(n)} \equiv 1^k\ (mod\ n) \quad \text{atau} \quad a^{k \cdot \phi(n)} \equiv 1\ (mod\ n) \tag{2}$$

Selanjutnya, jika a diganti dengan plainteks m, maka diperoleh:

$$m^{k \cdot \phi(n)} \equiv 1\ (mod\ n) \tag{3}$$

Dengan menggunakan sifat kekongruenan lainnya, yakni jika $a \equiv b\ (mod\ n)$, maka $ac \equiv bc\ (mod\ n)$, apabila persamaan (3) dikali m maka:

$$m^{k \cdot \phi(n)+1} \equiv m\ (mod\ n) \tag{4}$$

Misalkan terdapat dua bilangan bulat e dan d yang memenuhi:

$$e \cdot d \equiv 1\ (mod\ \phi(n)) \tag{5}$$

atau dapat ditulis dalam bentuk persamaan:

$$e \cdot d = k \cdot \phi(n) + 1 \tag{6}$$

Jika nilai $k \cdot \phi(n) + 1$ disubstitusikan ke pangkat pada persamaan (4), maka didapatkan:

$$m^{e \cdot d} \equiv m\ (mod\ n) \tag{7}$$

Persamaan (7) dapat ditulis kembali menjadi:

$$(m^e)^d \equiv m\ (mod\ n) \tag{8}$$

Persamaan (8) berarti bahwa plainteks m yang dipangkatkan dengan e, lalu hasilnya dipangkatkan lagi dengan d, akan menghasilkan ulang plainteks m. Berdasarkan persamaan (8), fungsi enkripsi dan dekripsi dapat diformulasikan sebagai berikut:

$$\text{Fungsi enkripsi: } c = E_e(m) = m^e \ (mod\ n) \tag{9}$$

$$\text{Fungsi dekripsi: } m = D_d(c) = c^d \ (mod\ n) \tag{10}$$

Karena $m^d \ (mod\ n) = (m + jn)^d \ (mod\ n)$ untuk sebarang bilangan bulat j, maka setiap plainteks $\{m, (m+n), (m+2n), ...\}$ akan menghasilkan cipherteks yang sama. Dengan kata lain, transformasinya dari banyak ke satu. Agar transformasinya bijektif, maka m harus dibatasi pada interval $[1, n-1]$.

2.3 Persamaan Diophantine Linear

Persamaan Diophantine adalah sembarang persamaan yang memiliki satu atau lebih variabel yang solusinya merupakan bilangan bulat [11]. Dalam konteks algoritma RSA, bentuk yang digunakan adalah persamaan Diophantine linear dua variabel yang memiliki bentuk umum sebagai berikut:

$$Ax + By = C \tag{11}$$

dengan $A, B, C \in \mathbb{Z}$ dan $x, y \in \mathbb{Z}$ adalah solusi.

Teorema. Persamaan Diophantine linear $Ax + By = C$ memiliki penyelesaian bilangan bulat jika $\text{FPB}(A, B) \mid C$.

Bukti. Misalkan $\text{FPB}(A, B) = w$. Maka secara definisi berlaku $w \mid A$ dan$w \mid B$. Dengan demikian, terdapat bilangan bulat u dan v sehingga:

$$A = uw \tag{12}$$

$$B = vw \tag{13}$$

Jika persamaan (12) dikalikan dengan x maka:

$$Ax = uwx \tag{14}$$

demikian pula, jika persamaan (13) dikalikan dengan y, diperoleh:

$$By = vwy \tag{15}$$

Menjumlahkan persamaan (14) dan (15) diperoleh:

$$Ax + By = (ux + vy)w \tag{16}$$

Sementara itu, bentuk umum persamaan Diophantine linear $Ax + By = C$. Berdasarkan persamaan (16) dapat disimpulkan bahwa:

$$C = (ux + vy)w \tag{17}$$

Karena $(ux + vy)$ adalah bilangan bulat, maka persamaan (17) memenuhi definisi keterbagian. Dengan kata lain, $w \mid C$ atau $\text{FPB}(A, B) \mid C$ ■.

2.4 Invers Modulo

Invers modulo dari suatu bilangan a terhadap modulo m adalah bilangan bulat x yang memenuhi [12]:

$$a \cdot x \equiv 1 \ (mod\ n) \tag{18}$$

Invers modulo memiliki solusi jika dan hanya jika $\text{FPB}(a,\ m) = 1$ [13]. Dalam konteks algoritma RSA invers modulo sangat penting karena digunakan untuk menentukan nilai dari kunci privat d dari kunci publik e dan $\phi(n)$. Secara eksplisit, nilai d diperoleh dari membagi e dengan persamaan (5) maka:

$$d \equiv e^{-1} \ (mod\ \phi(n)) \tag{19}$$

2.5 Algoritma Euclid

Algoritma Euclid merupakan salah satu cara yang efisien untuk menemukan faktor persekutuan terbesar suatu bilangan bulat positif. Misal a dan b bilangan bulat positif bentuk umum algoritma Euclid [14]:

$$\begin{array}{rcll} a & = & q_1 b + r_1 & 0 < r_1 < b \\ b & = & q_2 r_1 + r_2 & 0 \leq r_2 < r_1 \\ r_1 & = & q_3 r_2 + r_3 & 0 \leq r_3 < r_2 \\ \vdots & = & \vdots & \vdots \\ r_{n-2} & = & q_n r_{n-1} + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} & = & q_{n+1} r_n + 0 & \end{array}$$

Algoritma Euclid tidak hanya digunakan untuk menghitung faktor persekutuan terbesar suatu bilangan bulat positif. Algoritma ini juga berperan penting dalam penyelesaian persamaan Diophantine linear, yaitu persamaan linear dua variabel yang memiliki koefisien dan solusi dalam himpunan bilangan bulat. Persamaan tersebut dinyatakan sebagai [15] :

$$Ax + By = \text{FPB}(A, B) \tag{20}$$

Jika $\text{FPB}(A, B) = 1$, maka nilai x merupakan invers modulo dari A $(mod\ B)$ dan sebaliknya, y merupakan invers modular dari B $(mod\ A)$.

3 Hasil Utama

Setelah memahami kerangka teoretis dari algoritma RSA dan persamaan Diophantine linear, bagian ini menyajikan kontribusi utama dari penelitian. Fokus pembahasan diarahkan pada formulasi matematis dari proses pembangkitan kunci privat sebagai permasalahan persamaan Diophantine linear. Pembahasan ini dilengkapi dengan algoritma penyelesaian serta ilustrasi numerik yang bertujuan untuk memperjelas keterkaitan antara aspek teoretis dan penerapannya dalam konteks algoritma RSA. Dengan memahami dasar-dasar teori bilangan dan algoritma RSA, kita dapat menyusun ulang proses pembentukan kunci privat dalam bentuk yang lebih eksplisit secara matematis, yaitu menggunakan persamaan Diophantine linear.

Untuk itu, bagian berikut menguraikan bagaimana persamaan kongruensi dalam algoritma RSA dapat ditransformasikan menjadi bentuk persamaan Diophantine linear.

3.1 Transformasi Persamaan Kongruensi menjadi Persamaan Diophantine Linear

Dalam algoritma RSA, Kunci privat d diperoleh dengan menyelesaikan persamaan (6) yang diubah menjadi bentuk persamaan Diophantine linear dua variabel:

$$e \cdot d - k \cdot \phi(n) = 1$$

yang merupakan bentuk umum:

$$Ax + By = C$$

dengan $A = e,\ B = \phi(n)$, dan $C = 1$. Persamaan diatas memiliki solusi bilangan bulat d dan $(-k)$ jika dan hanya jika $\text{FPB}(e,\ \phi(n)) = 1$. Untuk memverifikasi pendekatan ini secara numerik, berikut disajikan satu contoh kasus sederhana.

3.2 Penerapan Langsung: Contoh Kasus Numerik

Misalkan dipilih dua bilangan prima:

$$p = 2027 \quad \text{dan} \quad q = 2029$$

sehingga:

$$n = p \cdot q = 4112783$$

$$\phi(n) = (p-1)(q-1) = 4108728$$

Dipilih nilai $e = 127$ yang memenuhi $(1 < e < \phi(n))$. Untuk memastikan bahwa FPB$(127, 4108728) = 1$, dilakukan pemeriksaan menggunakan algoritma Euclid:

$$\begin{aligned} 4108728 &= 127 \cdot 32352 + 24 \\ 127 &= 24 \cdot 5 + 7 \\ 24 &= 7 \cdot 3 + 3 \\ 7 &= 3 \cdot 2 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

Karena hasil akhir dari algoritma Euclid adalah 1, maka dapat disimpulkan bahwa FPB$(127,\ 4108728) = 1$, sehingga persamaan Diophantine linear yang bersesuaian dijamin memiliki solusi dalam himpunan bilangan bulat.
Dengan adanya jaminan solusi tersebut, langkah berikutnya adalah menentukan nilai kunci privat secara eksplisit melalui penyelesaian persamaan Diophantine. Proses ini dilakukan dengan metode substitusi balik berdasarkan hasil dari algoritma Euclid sebelumnya.

3.3 Menyelesaikan Persamaan Diophantine

Dilakukan substitusi balik dari algoritma Euclid:

$$127 \cdot d - k \cdot 4108728 = 1$$

Langkah-langkah substitusi balik:

$$\begin{aligned} 1 &= 7 - 3 \cdot 2 \\ &= (127 - 24 \cdot 5) - 2(24 - 7 \cdot 3) \\ &= 127 - 24 \cdot 5 - 2 \cdot 24 + 7 \cdot 6 \\ &= 127 - 24 \cdot 7 + 6(127 - 24 \cdot 5) \\ &= 127 - 24 \cdot 7 + 6 \cdot 127 - 24 \cdot 30 \\ &= (1+6)127 - (30+7)24 \\ &= 7 \cdot 127 - 37 \cdot 24 \\ &= 7 \cdot 127 - 37(4108728 - 127 \cdot 32352) \\ &= 7 \cdot 127 - 37 \cdot 4108728 + 127 \cdot 1197024 \\ &= (7 + 1197024)127 - 37 \cdot 4108728 \\ &= 1197031 \cdot 127 - 37 \cdot 4108728 \end{aligned}$$

Maka diperoleh nilai $d = 1197031$ dan $k = -37$ sebagai solusi dari persamaan Diophantine linear. Untuk memastikan bahwa nilai kunci privat tersebut benar-benar valid dan dapat digunakan dalam praktik, langkah selanjutnya adalah melakukan proses enkripsi dan dekripsi terhadap sebuah contoh plainteks sederhana. Proses validasi ini bertujuan untuk membuktikan bahwa kunci privat hasil penyelesaian persamaan Diophantine bekerja sesuai dengan prinsip dasar algoritma RSA.

3.4 Validasi Melalui Proses Enkripsi dan Dekripsi Algoritma RSA

Misal plainteks yang digunakan adalah "Hai", yang dalam kode ASCII 8-bit diwakili oleh:

Tabel 1: Konversi Alfabet ke ASCII 8-bit

Alfabet	ASCII 8-bit
H	072
a	097
i	105

Proses Enkripsi

Melakukan enkripsi plainteks dengan menggunakan persamaan (9), hasil enkripsi:

$$c_1 = 072^{127} \ (mod\ 4112783) = 3134209$$
$$c_2 = 097^{127} \ (mod\ 4112783) = 3840137$$
$$c_3 = 105^{127} \ (mod\ 4112783) = 2783386$$

Proses Dekripsi

Melakukan dekripsi cipherteks dengan menggunakan persamaan (10), hasil dekripsi:

$$m_1 = 3134209^{1197031} \ (mod\ 4112783) = 072$$
$$m_2 = 3840137^{1197031} \ (mod\ 4112783) = 097$$
$$m_3 = 2783386^{1197031} \ (mod\ 4112783) = 105$$

Dengan demikian diperoleh kembali plainteks asli "Hai", yang menunjukkan bahwa nilai d yang diperoleh dari penyelesaian persamaan Diophantine linear valid digunakan sebagai kunci privat dalam algoritma RSA.

4 Kesimpulan

Penelitian ini bertujuan untuk menjelaskan secara formal bagaimana persamaan Diophantine linear berperan dalam proses pembangkitan kunci privat pada algoritma RSA. Permasalahan ini penting untuk dipahami karena struktur matematis di balik algoritma RSA menjadi landasan utama dalam menjaga keamanan data digital di era modern.

Hasil utama yang diperoleh menunjukkan bahwa persamaan kongruensi yang digunakan dalam pembentukan kunci privat algoritma RSA dapat diubah menjadi bentuk persamaan Diophantine linear dua variabel. Penyelesaian persamaan Diophantine linear dua variabel, dilakukan melalui algoritma Euclid dan substitusi balik, sehingga menghasilkan nilai kunci privat yang valid digunakan dalam proses dekripsi. Studi kasus yang disertakan menunjukkan bahwa proses enkripsi dan dekripsi berhasil dilakukan dengan benar menggunakan kunci hasil formulasi tersebut.

Kontribusi utama dari kajian ini adalah formalisasi eksplisit dari langkah pembangkitan kunci privat algoritma RSA sebagai persoalan penyelesaian persamaan Diophantine linear. Hal ini memberikan dasar teoritis yang kuat dan memperjelas hubungan antara teori bilangan dengan algoritma kriptografi modern, khususnya dalam konteks algoritma RSA.

Penelitian ini bersifat teoretis dan belum mengeksplorasi efisiensi algoritmik pada skala bilangan besar yang digunakan dalam kriptografi praktis. Oleh karena itu, arah penelitian selanjutnya dapat diarahkan pada analisis kompleksitas algoritma Euclid dalam konteks algoritma RSA modern, serta pengembangan pendekatan yang lebih efisien atau adaptif dalam menyelesaikan persamaan Diophantine pada kriptografi berbasis bilangan bulat besar.

Pernyataan Kontribusi Penulis (CRediT)

Penulis Pertama: Konseptualisasi, Metodologi dan Penulisan–Draf Awal.
Penulis Kedua: Analisis Formal, Penulisan–Telaah, Validasi dan Penyuntingan.

Deklarasi Penggunaan AI atau Teknologi Berbasis AI

"Model ChatGPT digunakan untuk koreksi struktur kalimat dan koreksi skrip latex."

Deklarasi Konflik Kepentingan

"Penulis menyatakan tidak ada konflik kepentingan."

Daftar Pustaka

[1] R. Pamungkas and F. W. Z. Zaney, "Penerapan hashing sha1 dan algoritma asimetris rsa untuk keamanan data pada sistem informasi berbasis web," *RESEARCH: Journal of Computer, Information System & Technology Management*, vol. 4, no. 1, p. 84, 2021. DOI: https://doi.org/10.25273/research.v4i1.9099.

[2] D. N. Simatupang and E. Ardhianto, "Penambahan aspek integritas informasi pada model enkripsi light weight parallel encryption with digit arithmetic of covertext menggunakan algoritma sha-1," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 3, pp. 4718–4726, 2025. DOI: https://doi.org/10.36040/jati.v9i3.13539.

[3] T. H. Saputro, N. H. Hidayati, and E. I. H. Ujianto, "Survei tentang algoritma kriptografi asimetris," *Jurnal Informatika Polinema*, vol. 6, no. 2, pp. 67–72, 2020. DOI: https://doi.org/10.33795/jip.v6i2.345.

[4] Y. Zhou, "Role of linear diophantine equations in rsa encryption," *Theoretical and Natural Science*, vol. 42, no. 1, pp. 108–111, 2024. DOI: 10.54254/2753-8818/42/20240670.

[5] W. Trappe and L. C. Washington, *Introduction to Cryptography with Coding Theory*, 2nd ed. Pearson Prentice Hall, 2006.

[6] M. Deora and P. Pal, *An average case efficient algorithm for solving two-variable linear diophantine equations*, 2025. arXiv: 2409.14052 [cs.CR]. Available online.

[7] Y. A. Pradana, L. P. Dewi, M. A. Rahmah, A. Wijanarko, N. Ishartono, and D. A. Kusumaningtyas, "Penyelesaian aplikasi persamaan diophantine dengan algoritma euclid," *Jurnal Keilmuan Dan Keislaman*, pp. 10–18, 2024. DOI: 10.23917/jkk.v3i1.173.

[8] R. Munir, *Kriptografi*, 2nd ed. Bandung: Informatika Bandung, 2019.

[9] K. Assa-Agyei and F. Olajide, "A comprehensive evaluation of the rivest-shamir-adleman (rsa) algorithm performance on operating systems using different key bit sizes," *International Journal of Computer Applications*, vol. 185, no. 19, 2023. DOI: 10.5120/ijca2023922884. Available online.

[10] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978. DOI: 10.1145/359340.359342.

[11] S. Al Jupri, *Dasar-Dasar Teori Bilangan*. Yrama Widya, 2020. Available online.

[12] K.-D. Crisman, *Number Theory: In Context and Interactive*, 2024/6 Edition. American Institute of Mathematics / Gordon College (OER), 2024. Available online.

[13] D. R. Kandel, "Euclid's algorithm and its role in solving modular multiplicative inverse," *Kaumodaki: Journal of Multidisciplinary Studies*, vol. 4, no. 1, pp. 85–95, 2024. DOI: 10.3126/kdk.v4i1.64567.

[14] D. M. Burton, *Elementary Number Theory*, 7th ed. McGraw-Hill Higher Education, 2010.

[15] K. H. Rosen, *Elementary Number Theory and Its Applications*. Addison-Wesley, 1984.