International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 04 April 2026
DOI: 10.47191/ijcsrr/V9-i4-49, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

The Multi-Prime RSA Permutation Crypto System Based on Clear Ring

Bambang Irawanto[1], Benediktus Panji Pradipta[2], Nikken Prima Puspita[3*]
[1,2,3] Department of Mathematics, Faculty of Science and Mathematics, Universitas Diponegoro, Jl. Prof. Jacub Rais, Semarang, 50275, Indonesia

ABSTRACT: Cryptography secures information through encryption, allowing only authorized access. The RSA algorithm, which relies on the difficulty of factoring $n = pq$ where p and q are primes, is a popular public-key cryptosystem. Advances in factorization techniques and computing power necessitate improvements to methods for enhanced security. This study proposes a multi-prime RSA permutation cryptosystem based on the algebraic structure of a clear ring as a modification of RSA. It uses three primes p_1, p_2, p_3 to form modulus $n = p_1 p_2 p_3$, increasing modulus complexity and thus security. Permutation is applied in binary code form to produce more random ciphertext, alongside the application of a clear ring structure, specifically, the ring of integers modulo 256 with addition and multiplication modulo 256 based on ASCII. This ring allows each element to be expressed as a sum of a unit and a regular unit. The algorithm strengthens key generation and creates varied representations for the same plaintext through unit and regular unit addition, complicating cryptanalysis. Permutation further randomizes ciphertext. However, the method requires careful implementation to avoid errors. This innovation supports digital security.

KEYWORDS: Clear Ring, Cryptography, Permutation, Ring, RSA, RSA Multi-Prime.

INTRODUCTION

The development of technology in the current digital era is increasingly rapid in various aspects of life, such as communication, education, economy, social, and government. This is inseparable from the role of the internet, which acts as the main driver in accelerating the flow of information and communication, data transfer, as well as various services and knowledge with unlimited access. Based on survey results released by APJII (Asosiasi Penyelenggara Jasa Internet Indonesia), the number of internet users in Indonesia in 2024 reached 221.6 million people, with a percentage of 79.5% [1]. Meanwhile, in early 2025, it surpassed 5.56 billion people, representing a 1.7% increase in internet users out of the total world population [2]. However, data security has become a crucial issue alongside the increase in internet usage. The exchange of critical information through internet connections can lead to vulnerabilities regarding data leaks to irresponsible parties [3]. Data leaks have potential to cause serious losses, such as material loss, reputational damage, invasion of individual privacy, identity theft, and other manipulations [4].

Various information leakage cases in Indonesia pose a serious challenge to data security. In 2024, there was a leak case at the National Data Center (PDN) due to weak infrastructure and cyber security systems in the Indonesian government, where security gaps were not well anticipated. Furthermore, the BPJS Kesehatan data leak in 2021 was one of the largest incidents, where approximately 279 million population data records were successfully breached [5]. Additionally, around 21,769,496 email accounts in Indonesia were compromised in 2024, placing Indonesia 3rd in ASEAN for the highest number of data leak cases [6]. Thus, personal data protection has become an urgent global challenge. Data leak cases in various fields have become a serious concern requiring a firm, responsive, and effective response [7].

One approach to maintaining data security is through cryptography. The term cryptography comes from the Greek words crypto (secret) and graphia (writing). Cryptography is the science that studies encryption techniques or the application of algorithms so that information can only be read by authorized parties [8]. In general, cryptography is divided into two types: symmetric cryptography and asymmetric (public key) cryptography. One of the most famous and widely used public-key cryptographic algorithms is the RSA (Rivest – Shamir – Adleman) algorithm. RSA security depends on the difficulty of factoring a large number n, which is the product of two prime numbers. However, if n has a length of 256 bits or less, n can be factored in a few hours using a computer and freely available programs. Consequently, the security level of the RSA algorithm is declining in this modern computing era. Therefore, a modification of the RSA algorithm is required to increase the encryption security level.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 04 April 2026
DOI: 10.47191/ijcsrr/V9-i4-49, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

Based on these problems, this research aims to modify the RSA algorithm into a permutation multi-prime RSA cryptosystem based on algebraic structure of clear ring. This modification uses three prime numbers to form the modulus to increase factorization difficulty and applies permutation in the form of binary code to generate a more random ciphertext. Furthermore, this algorithm utilizes the clear ring algebraic structure of integers modulo 256 based on the American Standard Code for Information Interchange (ASCII) to expand the plaintext representation. This research is expected to strengthen the cryptographic security of the RSA algorithm while reducing the risk of data leaks caused by the weaknesses of classic RSA. Furthermore, this innovation is expected to support the achievement of SDGs point 9 regarding industry, innovation, and infrastructure through the development of a more innovative information security system.

METHODOLOGY

This research relates to cryptography, specifically the multi-prime RSA algorithm and the theory of clear ring algebraic structures. Furthermore, an analysis was performed to identify the weaknesses of the multi-prime RSA algorithm and modify it into a new algorithm called Permutation multi-prime RSA based on the clear ring algebraic structure. The steps of this research are as follows:

1. Studying the importance of information security in the context of modern cryptography.
2. Collecting references and studying cryptographic concepts, including their terms and types.
3. Reviewing the multi-prime RSA algorithm along with its advantages and disadvantages.
4. Studying the clear ring structure and permutation group concepts, including their relevant properties.

Designing a modification of the multi-prime RSA algorithm by converting each plaintext element into a clear element, as well as adding the concept of permutation groups to the encryption and decryption processes, thus forming a new algorithm called permutation multi-prime RSA based on the clear ring algebraic structure.

RESULTS AND DISCUSSION

This chapter discusses the multi-prime RSA permutation cryptosystem based on the algebraic structure of the clear ring, which includes the encryption process, the decryption process, as well as the advantages and disadvantages of the cryptosystem.

The Multi-Prime Permutation RSA Cryptosystem Based on Clear Ring

The multi-prime RSA permutation cryptosystem based on clear rings is a development of the RSA algorithm that aims to strengthen security. Messages to be encrypted with this cryptosystem are not processed directly, but are first represented in a clear ring structure where each element can be expressed as the sum of a unit element and a regular unit. The following are the definitions of unit elements and regular unit elements.

Definition 1. [9] Let $(\mathrm{R}, +, \cdot)$ be a ring with a multiplicative identity 1_{R}. An element $\mathrm{u} \in \mathrm{R}$ is called a *unit* if there exists an element $\mathrm{s} \in \mathrm{R}$ such that $\mathrm{us} = \mathrm{su} = 1_{\mathrm{R}}$. Furthermore, the set of all units in R is denoted by $U(R)$.

Definition 2. [9] Let $(\mathrm{R}, +, \cdot)$ be a ring with unity 1_{R}. An element $\mathrm{v} \in \mathrm{R}$ is called a **regular unit element** if there exists $\mathrm{u} \in \mathrm{U(R)}$ such that $\mathrm{v} = \mathrm{vuv}$. Furthermore, the set of all regular unit elements in R is denoted by $U_{reg}(R)$.

After understanding the definitions of unit elements and regular unit elements, a special algebraic ring structure called a clear ring is introduced.

Definition 3. [10] Let $(\mathrm{R}, +, \cdot)$ be a ring with identity element 1_{R}. The ring R is said to be *clear* if for every element $\mathrm{r} \in \mathrm{R}$, there exist $\mathrm{u} \in \mathrm{U(R)}$ and $\mathrm{v} \in \mathrm{U_{reg}(R)}$ such that $\mathrm{r} = \mathrm{u} + \mathrm{v}$.

In cryptography, the algebraic structure of a clear ring is implemented in the multi-prime RSA cryptosystem and permutation cipher cryptosystem. The following are the definitions of the multi-prime RSA cryptosystem and the permutation cipher cryptosystem.

Definition 4. [11] A multi-prime RSA cryptosystem is an asymmetric cryptographic scheme derived from the standard RSA, constructed by using more than two prime numbers in the generation of the private key.

Definition 5. [12] Let m be a positive integer. Given a plaintext set $(\mathcal{P})$, a ciphertext set $(\mathcal{C})$, and a key set $(\mathcal{K})$, each consisting of all text blocks of length m characters. For a permutation key π, the encryption and decryption processes are defined as follows:

$$e_{\pi}(x_1, \dots, x_m) = (x_{\pi(1)}, \dots, x_{\pi(m)}) \quad (1)$$

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 04 April 2026
DOI: 10.47191/ijcsrr/V9-i4-49, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

and

$$d_\pi(y_1, \dots, y_m) = (y_{\pi^{-1}(1)}, \dots, y_{m^{-1}(1)}), \quad (2)$$

where π^{-1} denotes the inverse permutation of π.

Algorithm of Multi-Prime Permutation RSA Cryptosystem Based on Clear Ring

The combination of the clear ring algebraic structure implemented in the multi-prime RSA cryptosystem and in the permutation cipher cryptosystem motivates the development of a new cryptographic innovation, namely the clear-ring–based multi-prime RSA permutation cryptosystem.

Before the encryption process is carried out, a key must be generated for message security. The steps in the key generation algorithm in the multi-prime RSA permutation cryptosystem based on the clear ring algebraic structure are as follows.

1. The process begins by selecting three prime numbers p_1, p_2, and p_3.
2. The product of these three primes yields the value n, which can be written as $n = p_1 \times p_2 \times p_3$.
3. The Euler totient function $\varphi(n)$ is computed as $(p_1 - 1)(p_2 - 1)(p_3 - 1)$, written as $\varphi(n) = (p_1 - 1)(p_2 - 1)(p_3 - 1)$.
4. A number e is chosen such that $gcd(e, \varphi(n)) = 1$.
5. The value d is determined as the inverse of e modulo $\varphi(n)$, that is $d \equiv e^{-1}(mod\ \varphi(n))$.
6. The key generation produces a public key pair (n, e) and a private key pair (n, d).

After understanding the steps of the key generation algorithm, this can be clarified in **Example 1.**

Example 1. Bob generates a multi-prime RSA key by selecting three $p_1 = 13$, $p_2 = 23$, and $p_3 = 29$, which produce the modulus $n = p_1 \times p_2 \times p_3 = 8671$ and Euler's totient $\varphi(n) = (p_1 - 1)(p_2 - 1)(p_3 - 1) = 7392$. He chooses the public exponent $e = 19$, satisfying $gcd(19,7392) = 1$. The private exponent d is defined by the modular inverse $19d \equiv 1(mod\ 7392)$, yielding $d = 7003$. Consequently, the resulting key pair is the public key $(e, n) = (19,8671)$ and the private key $(d, n) = (7003,8671)$.

The encryption function of the multi-prime RSA permutation cryptosystem over the clear algebraic ring is defined for a plaintext message M by

$$C = E(M) = M^e\ mod\ 256,$$

where M denotes the plaintext to be encrypted, e is the public exponent used in the encryption process, and $n = p_1 \times p_2 \times p_3$ is the modulus formed from three distinct prime numbers p_1, p_2, and p_3. The value C represents the resulting ciphertext. Subsequently, the ciphertext C is permuted using a permutation function π defined on the ciphertext block, producing

$$C' = \pi(C).$$

In general, the permutation function π is a bijection $\pi : \{1, 2, \dots, t\} \to \{1, 2, \dots, t\}$, that rearranges the positions of ciphertext elements according to a specified pattern in order to enhance the secrecy of the encrypted output.

The steps in the encryption algorithm in the multi-prime RSA permutation cryptosystem based on the ring clear algebraic structure are as follows.

1. The encryption process begins by selecting three distinct primes p_1, p_2, and p_3, whose product forms the modulus $n = p_1 \times p_2 \times p_3$with Euler's totient $\varphi(n) = (p_1 - 1)(p_2 - 1)(p_3 - 1)$.
2. A public exponent e is chosen such that $1 < e < \varphi(n)$ and $gcd(e, \varphi(n)) = 1$.
3. The private exponent d is then computed as $d \equiv e^{-1}(mod\ \varphi(n))$. The pair (e, n) serves as the public key and (d, n) as the private key.
4. The plaintext message M is expressed as a sequence of characters $M = (m_1, m_2, \dots, m_t)$. Each character m_i is represented by its ASCII numerical value and may be viewed as an element of the ring $\mathbb{Z}_{256}$. Thus, each m_i can be written as $m_i = u_i + r_i$, where u_i is the unit element and r_i is the regular element of the ring, for $i = 1,2,3, \cdots, t$.
5. Each pair (u_i, r_i) is encrypted using the multi-prime RSA function defined by $C_{u_i} = u_i^e\ mod\ n$ and $C_{r_i} = r_i^e\ mod\ n$.
6. The resulting ciphertext is the sequence $C = (C_{u_1}, C_{r_1}, C_{u_2}, C_{r_2}, \dots, C_{u_t}, C_{r_t})$.
7. The combined ciphertext C is converted into its HEX representation according to the ASCII table.
8. The HEX-encoded ciphertext is then processed by a permutation function $\pi : \{1, 2, \dots, t\} \to \{1, 2, \dots, t\}$, producing the final ciphertext $C' = \pi(C)$.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 04 April 2026
DOI: 10.47191/ijcsrr/V9-i4-49, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

To clarify the process in the encryption algorithm, here is **Example 2**, which explains the encryption process.

Example 2. In the presented encryption example, Alice sends the secret message "FIMNAS" to Bob using the RSA cryptosystem with a public key $(n, e) = (8671, 19)$ and a private key $(n, d) = (8671, 7003)$. The plaintext is first decomposed based on ASCII values into its unit elements u_i and regular elements r_i within the ring $(\mathbb{Z}_{256}, +_{256}, \cdot_{256})$. Each element is then encrypted separately, yielding the sequences C_{u_i} and C_{r_i}, which are combined to form the initial ciphertext block $\{01, FD, 19, 00, 95, 00, DB, 33, C1, 00, 4B, 00\}$ in hexadecimal format. Subsequently, a permutation function $\pi(i) = 5 \cdot (i-1) + 1 \; mod \; 24 + 1$ is applied to this block, resulting in the final permuted ciphertext $009035100CB00210D08F05E$, which is transmitted to Bob.

The decryption function of the multi-prime RSA cryptosystem is based on the inverse function of the encryption function where the decryption of the ciphertext C is defined as follows:

$$P = D(C') = C'^{d} \; mod \; n, \qquad (3)$$

where:
P is the original plaintext before encryption.
d is calculated from the three prime numbers used in the decryption process.
$n = p_1 \times p_2 \times p_3$ are the results of the three largest prime numbers for the private keys p_1, p_2, dan p_3,
C' is the result of the encryption function (ciphertext) that contains the encrypted message.

Before the decryption process is carried out, the ciphertext C′ is first restored to its original form by applying the inverse of the permutation function π used during the encryption stage. Since the permutation function π is bijective, there exists an inverse π^{-1} that can be used to recover the original ordering of the ciphertext. Thus, the initial ciphertext can be obtained through

$$C = \pi^{-1}(C'). \qquad (4)$$

The steps for the multi-prime RSA decryption algorithm based on the implementation of a modular exponentiation technique on two numbers are as follows:

1. The ciphertext C'received from the sender is in the form of a hexadecimal string, which must be converted to its integer form P.
2. The integer C' is then converted to its original form, which is an ASCII string.
3. The inverse function π^{-1} is used to perform modular arithmetic on the ciphertext C' to return to its original form, $C = \pi^{-1}(C')$
4. The ciphertext C consists of message components (C_{u_i}, C_{r_i}) such that where $i = 1, 2, \dots, t$, each component represents the result of the encryption of the element u_i and the regular element r_i.
5. The decryption process for each component is performed using the private key (d, n) through the decryption function, which is:

$$u_i = C_{u_i}^{d} \; mod \; n \qquad (5)$$

and

$$r_i = C_{r_i}^{d} \; mod \; n. \qquad (6)$$

for each $i = 1, 2, \dots, t$.

6. The decrypted components u_i and r_i are then recombined to reconstruct each plaintext character using

$$m_i = u_i + r_i \; mod \; 256 \qquad (7)$$

for each $i = 1, 2, \dots, t$.

7. The values m_i obtained are then converted back into their corresponding ASCII characters to reconstruct the original message $M = (m_1, m_2, \dots, m_t)$.
8. Thus, the decryption process successfully recovers the original message M.

To better understand the decryption process, **Example 3** is provided below.

Example 3. The process begins by determining the inverse of the permutation function $\pi(i) = 5 \cdot (i-1) + 1 \; mod \; 24 + 1$. Since $\gcd(5,24) = 1$, the modular inverse of 5 modulo 24 exists and is found to be 5 via the Extended Euclidean Algorithm, yielding the inverse permutation $\pi^{-1}(i) = 5(i-2) \; mod \; 24 + 1$. Applying π^{-1} to the received

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 04 April 2026
DOI: 10.47191/ijcsrr/V9-i4-49, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

ciphertext $009035100CB00210D08F05E$ reverses the permutation, producing the sequence $P = \{01, FD, 19, 00, 95, 00, DB, 33, C1, 00, 4B, 00\}$ in hexadecimal. This sequence is then converted back into its decimal form $\{1, 253, 25, 0, 149, 0, 219, 51, 193, 0, 75, 0\}$. Subsequently, the original unit elements u_i and regular elements r_i are recovered by computing $u_i = C_{u_1}^d \ mod\ 256$ dan $r_i = C_{r_i}^d \ mod\ 256$ using the private key $d = 7003$. Finally, the original plaintext characters are reconstructed by summing the corresponding unit and regular elements ($m_i = u_i + r_i$), which yields the decimal sequence $\{70, 73, 77, 78, 65, 83\}$. Converting these values back to ASCII characters successfully retrieves the original plaintext: FIMNAS.

The advantage of the multi-prime permutation RSA cryptosystem based on the algebraic structure of the clear ring lies in the use of three distinct prime numbers in constructing the modulus $n = p_1 \times p_2 \times p_3$, which significantly increases the difficulty of factorization. In addition, the implementation of a clear ring structure and permutation, which allows each plaintext character to be represented as a combination of unit elements and regular units, produces ciphertext with higher randomness and variability. This mechanism strengthens the system's resistance to cryptanalysis attacks.

The drawback of this cryptosystem lies in the increased complexity of the encryption and decryption processes due to the representation of clear ring elements and ciphertext permutation, which may reduce system performance when applied to large data sets. Furthermore, the use of permutation functions and their inverse requires high precision since minor index errors may result in invalid decryption outputs

CONCLUSION

This research demonstrates that the modification of the classical RSA algorithm into a multi-prime permutation RSA algorithm based on a clear ring can enhance encryption security. The modification employs three prime numbers $p_1, p_2, dan\ p_3$, generating a more complex modulus that is considerably more difficult to factor. Moreover, the algorithm utilizes the algebraic structure of the clear ring $(\mathbb{Z}_{256}, +_{256}, \cdot_{256})$, enabling diverse representations of identical plaintexts through varying combinations of unit and regular unit elements. The ciphertext permutation further increases randomness, making cryptanalysis significantly more challenging, with an estimated complexity of 40,320 trial permutations. However, this algorithm still exhibits a limitation: an error occurring in the generation of any key component will propagate to subsequent processes, resulting in incorrect final decryption. Nonetheless, this research contributes to the advancement of data security in modern cryptography, aligning with SDG point 9 on industry, innovation, and infrastructure.

REFERENCES

1. Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), "APJII: jumlah pengguna internet indonesia tembus 221 juta orang," 2024. [Online]. Available: https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internetindonesia-tembus-221-juta-orang. [Accessed: Sep. 13, 2025].
2. Kementerian Komunikasi dan Digital, "Komitmen pemerintah melindungi anak di ruang digital," 2025. [Online]. Available: https://www.komdigi.go.id/berita/artikel/detail/komitmen-pemerintah-melindungi-anak-di-ruang-digital. [Accessed: Sep. 13, 2025].
3. W. Widodo, R. Ardiyanto, and R. K. Hapsari, "Implementasi kriptografi dengan algoritma RSA pada aplikasi transfer data," in *Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika (SNESTIK)*, Surabaya, Indonesia: Institut Teknologi Adhi Tama Surabaya, 2023, pp. 34-40.
4. L. M. Aritonang, Zyetwill, and R. Handayani, "Analisis hukum terhadap kebocoran data pribadi dan penyalahgunaan identitas dalam perbankan berdasarkan undang-undang nomor 27 tahun 2022 tentang perlindungan data pribadi," *Journal of Multidisciplinary Research and Development*, vol. 7, no. 5, pp. 3146-3158, 2025.
5. D. A. Nugraha, R. Nurfitroh, N. D. Ul-Haq, P. R. Dika, and S. N. Lagontong, "Kebocoran data BPJS kesehatan: Ancaman terhadap keamanan informasi publik di era digital," *IPPSJ: Integrative Perspectives of Social and Science Journal*, vol. 2, no. 3, pp. 4685-4691, 2025.
6. B. R. Alfathi, "Indonesia peringkat ke-3 negara ASEAN dengan kebocoran data terbanyak," 2025. [Online]. Available: https://data.goodstats.id/statistic/indonesia-peringkat-ke-3-negara-asean-dengan-kebocoran-data-terbanyak-AtcAs. [Accessed: Sep. 14, 2025].

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 04 April 2026
DOI: 10.47191/ijcsrr/V9-i4-49, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

7. E. F. Pakpahan, L. R. Chandra, and A. A. Dewa, "Perlindungan hukum terhadap data pribadi dalam industri financial technology," *Veritas et Justitia*, vol. 6, no. 2, pp. 298–323, 2020.
8. B. R. Raharjo, *Keamanan Sistem Informasi*. Yayasan Prima Agus Teknik, 2021.
9. S. Wahyuni, I. E. Wijayanti, D. A. Yuwaningsih, and A. D. Hartanto, *Teori Ring dan Modul*. Yogyakarta, Indonesia: Gadjah Mada University Press, 2016.
10. B. V. Zabavsky, O. V. Domsha, and O. M. Romaniv, "Clear rings and clear elements," *Mathematical Studies*, vol. 55, pp. 3–9, 2021.
11. I. G. Talunohi, I. J. Lubis, Sutarman, and A. Candra, "Analisis perbandingan kinerja multi prime RSA dan multi power RSA," *CESS (Journal of Computing Engineering, System and Science)*, vol. 8, no. 2, pp. 576–582, 2023.
12. D. R. Stinson and M. Paterson, *Cryptography: Theory and Practice*, 4th ed. CRC Press, 2019.

Cite this Article: Irawanto, B., Pradipta, B.P., Puspita, N.P. (2026). The Multi-Prime RSA Permutation Crypto System Based on Clear Ring. International Journal of Current Science Research and Review, 9(4), pp. 2171-2176. DOI: https://doi.org/10.47191/ijcsrr/V9-i4-49