On a Generalization of RSA Crypto-system By Using 2-Cyclic Refined Integers

Hasan Sankari, Mohammad Abobala*

Tishreen University, Department of Mathematics, Latakia, Syria

Emails: Hasan2sankari@gmail.com; Mohammadabobala777@gmail.com

Abstract

The objective of this paper is to present a novel application of 2-cyclic refined integers to build a novel crypto scheme for the encryption and decryption of data and information based on the algebraic properties of 2-cyclic refined integers combined with RSA algorithm, where an improved version of RSA crypto-scheme will be established and applied to the security of information and data. On the other hand, we illustrate some examples and figures to show the validity and complexity of the algorithm.

Keywords: 2-cyclic refined integers; RSA; EL-Gamal; security system.

1. Introduction and preliminaries.

The reason behind mathematical cryptology is to keep media and message secret. In our days, the need for security arises too much, especially for social media accounts, multimedia exchange and all related subjects. In the literature, pure mathematics and number theory were very central in developing asymmetric crypto algorithms, that is because of the current complexity of many numbers theoretical problems. Asymmetric cryptography that uses the public key ideas was handled in the literature in terms of many algorithms based on mathematics and number theory [1-3], such as RSA, EL-Gamal, and Diffie-Hellman key exchange. In [4-7], many applications of non-classical extensions of number theory in cryptography were carried out, we can see neutrosophic version of RSA and El-Gamal algorithms and refined neutrosophic version of EL-Gamal algorithm to deal with neutrosophic data units and fuzzy matrices.

The concept of n-cyclic integers was defined in [8], and it was studied on a wide range by many authors, see [9-13]. In this paper, we use 2-cyclic refined number theoretical approach to build a new version of RSA algorithm, and we discuss its complexity compared to other algorithms.

Definition.
The 2- cyclic refined integer is defined as follows:
$x + yI_1 + zI_2; x, y, z \in Z$. it is denoted by $Z_2(I)$.
Addition:
$(x + yI_1 + zI_2) + (m + nI_1 + tI_2) = (x + m) + (y + n)I_1 + (z + t)I_2$.
Multiplication:
$(x + yI_1 + zI_2) \times (m + nI_1 + tI_2) = xm + (xn + ym + yt + zn)I_1 + (xt + yn + zm + zt)I_2$.
Definition.
For $L = l_0 + l_1I_1 + l_2I_2, s_0 + s_1I_1 + s_2I_2 \in Z_2(I)$, then $M = m_0 + m_1I_1 + m_2I_2$, we say:

1. $L \equiv S(mod\ M)$ if and only if:

$$\begin{cases} l_0 \equiv s_0(mod\ m_0) \\ l_0 + l_1 + l_2 \equiv (s_0 + s_1 + s_2)(mod\ m_0 + m_1 + m_2) \\ l_0 - l_1 + l_2 \equiv (s_0 - s_1 + s_2)(mod\ m_0 - m_1 + m_2) \end{cases}$$

2. $L > 0$ if and only if:

Doi : https://doi.org/10.54216/JCIM.120106
Received: December 24, 2022 Revised: February 15, 2023 Accepted: April 26, 2023

$$\begin{cases} l_0 > 0 \\ l_0 + l_1 + l_2 > 0 \\ l_0 - l_1 + l_2 > 0 \end{cases}$$

3. $L \geq S$ if and only if:

$$\begin{cases} l_0 \geq s_0 \\ l_0 + l_1 + l_2 \geq s_0 + s_1 + s_2 \\ l_0 - l_1 + l_2 \geq s_0 - s_1 + s_2 \end{cases}$$

4. $L^S = {l_0}^{s_0} + \frac{1}{2} I_1[(l_0 + l_1 + l_2)^{s_0+s_1+s_2} - (l_0 - l_1 + l_2)^{s_0-s_1+s_2}] + \frac{1}{2} I_1[(l_0 + l_1 + l_2)^{s_0+s_1+s_2} = (l_0 - l_1 + l_2)^{s_0-s_1+s_2} - 2{l_0}^{s_0}]$.

2. Main discussion.

Definition.

Let $X = x_0 + x_1 I_1 + x_2 I_2 \in Z_2(I)$, then we define the following special function $\emptyset^*: Z_2(I) \to Z$ such that:

$$\emptyset^*(X) = \begin{cases} \frac{1}{2}\emptyset(x_0) * \emptyset(x_0 + x_1 + x_2) * \emptyset(x_0 - x_1 + x_2);\ x_0 + x_1 + x_2 > 2 \text{ or } x_0 - x_1 + x_2 > 2 \\ \emptyset(x_0);\ x_0 + x_1 + x_2 = x_0 - x_1 + x_2 \leq 2 \end{cases}$$

Definition.

Let $X = x_0 + x_1 I_1 + x_2 I_2, Y = y_0 + y_1 I_1 + y_2 I_2 \in Z_2(I)$, then $gcd(X, Y) = 1$ if and only if:

$$\begin{cases} gcd(x_0, y_0) = 1 \\ gcd(x_0 + x_1 + x_2, y_0 + y_1 + y_2) = 1 \\ gcd(x_0 - x_1 + x_2, y_0 - y_1 + y_2) = 1 \end{cases}$$

Theorem.

If $gcd(X, M) = 1; M = m_0 + m_1 I_1 + m_2 I_2 \in Z_2(I)$, then $X^{\emptyset^*(M)} \equiv (1 \ mod\ M)$.

3. Mathematics in cryptography

Theoretical mathematics is an important resource of cryptography, as the most famous cryptographic algorithms with their symmetric and asymmetric types basically follow being generalized problems in traditional number theory and the theory of functions.

Concepts such as congruencies, Euler's function, and elliptic curves have been used in the construction and exchange of secret keys for the encryption and decryption process, perhaps the most prominent examples of this are asymmetric public-key encryption algorithms such as the RSA algorithm and the El-Gamal algorithm**.** Proceeding from this point, it can be said that by generalizing and expanding the integers used in the encryption and decryption process, it is possible to build encryption systems that generalize classical systems and are characterized by a higher degree of complexity and greater difficulty for attackers to obtain secret keys. So far, based on the latest published articles, three types of new numerical systems have been used that expand integers in the construction of new encryption algorithms based on previously known algorithms.
Neutrosophic integers, for example, are essentially an extended numerical system of partially ordered integers, possessing many characteristic properties in two dimensions. These numbers were used in the generalization of the RSA algorithm, and El-Gamal algorithm and have given good results in terms of the resulting complexity in the difficulty of breaking, and in the flow ability of the approval calculations.

On the other hand, refined neutrosophic integers and symbolic 2-plithogenic integers are essentially an extended numerical system of partially ordered integers, possessing many characteristic properties in three dimensions. These two novel sets provided good generalizations of classical RSA, and El-Gamal Systems, and these generalizations are more complex compared to classical algorithms, which implies more security for sharing information and data through the internet and unsafe channels.

3.1 The description of 2-cyclic refined RSA algorithm:

Suppose that we have two sides, a sender (F) and a recipient (E). Suppose that $M = m_0 + m_1 I_1 + m_2 I_2$ is the message that (F) decided to send it to (E).
(E) picks two positive 2-cyclic refined integers $P = p_0 + p_1 I_1 + p_2 I_2, Q = q_0 + q_1 I_1 + q_2 I_2$, with $p_0, q_0, p_0 + p_1 + p_2, q_0 + q_1 + q_2, p_0 - p_1 + p_2, q_0 - q_1 + q_2$ are large odd primes and then computes:
$N = PQ = p_0 q_0 + I_1(p_0 q_1 + p_1 q_0 + p_1 q_2 + p_2 q_1) + I_1(p_0 q_2 + p_2 q_0 + p_2 q_2 + p_2 q_1) = n_0 + n_1 I_1 + n_2 I_2$

Doi : https://doi.org/10.54216/JCIM.120106
Received: December 24, 2022 Revised: February 15, 2023 Accepted: April 26, 2023

$$\emptyset^*(N) = 2\emptyset^*(P).\emptyset^*(Q)$$
$$= \frac{1}{2}\emptyset(p_0) * \emptyset(p_0 + p_1 + p_2) * \emptyset(p_0 - p_1 + p_2)\emptyset(q_0) * \emptyset(q_0 + q_1 + q_2) * \emptyset(q_0 - q_1 + q_2)$$
$$= \frac{1}{2}(p_0 - 1)(p_0 + p_1 + p_2 - 1)(p_0 - p_1 + p_2 - 1)(q_0 - 1)(q_0 + q_1 + q_2 - 1)(q_0 - q_1 + q_2 - 1)$$

Then (E) picks $E = e_0 + e_1 I_1 + e_2 I_2$ with:

$$\begin{cases} 1 < e_0 < \emptyset^*(N), gcd\big(e_0, \emptyset^*(N)\big) = 1 \\ 1 < e_0 + e_1 + e_2 < \emptyset^*(N), gcd\big(e_0 + e_1 + e_2, \emptyset^*(N)\big) = 1 \\ 1 < e_0 - e_1 + e_2 < \emptyset^*(N), gcd\big(e_0 - e_1 + e_2, \emptyset^*(N)\big) = 1 \end{cases}$$

The public key is (E, N).

Now, (F) encrypts the message M as follows:

$$C \equiv M^E (mod\ N) = {m_0}^{e_0} (mod\ n_0)$$
$$+ \frac{1}{2} I_1 [(m_0 + m_1 + m_2)^{e_0 + e_1 + e_2} (mod\ n_0 + n_1 + n_2)$$
$$- (m_0 - m_1 + m_2)^{e_0 - e_1 + e_2} (mod\ n_0 - n_1 + n_2)]$$
$$+ \frac{1}{2} I_1 [(m_0 + m_1 + m_2)^{e_0 + e_1 + e_2} (mod\ n_0 + n_1 + n_2)$$
$$+ (m_0 - m_1 + m_2)^{e_0 - e_1 + e_2} (mod\ n_0 - n_1 + n_2) - 2{m_0}^{e_0} (mod\ n_0)]$$

The secret key is:

$$E^{-1} = {e_0}^{-1}\big(mod\ \emptyset^*(N)\big) + \frac{1}{2} I_1 \big[(e_0 + e_1 + e_2)^{-1}\big(mod\ \emptyset^*(N)\big) - (e_0 - e_1 + e_2)^{-1}\big(mod\ \emptyset^*(N)\big)\big]$$
$$+ \frac{1}{2} I_1 \big[(e_0 + e_1 + e_2)^{-1}\big(mod\ \emptyset^*(N)\big) - (e_0 - e_1 + e_2)^{-1}\big(mod\ \emptyset^*(N)\big)$$
$$- {e_0}^{-1}\big(mod\ \emptyset^*(N)\big)\big]$$

The recipient (E) decrypts the message by $M \equiv C^{E^{-1}} (mod\ N)$. The steps are declared in Figure 1 (a and b).

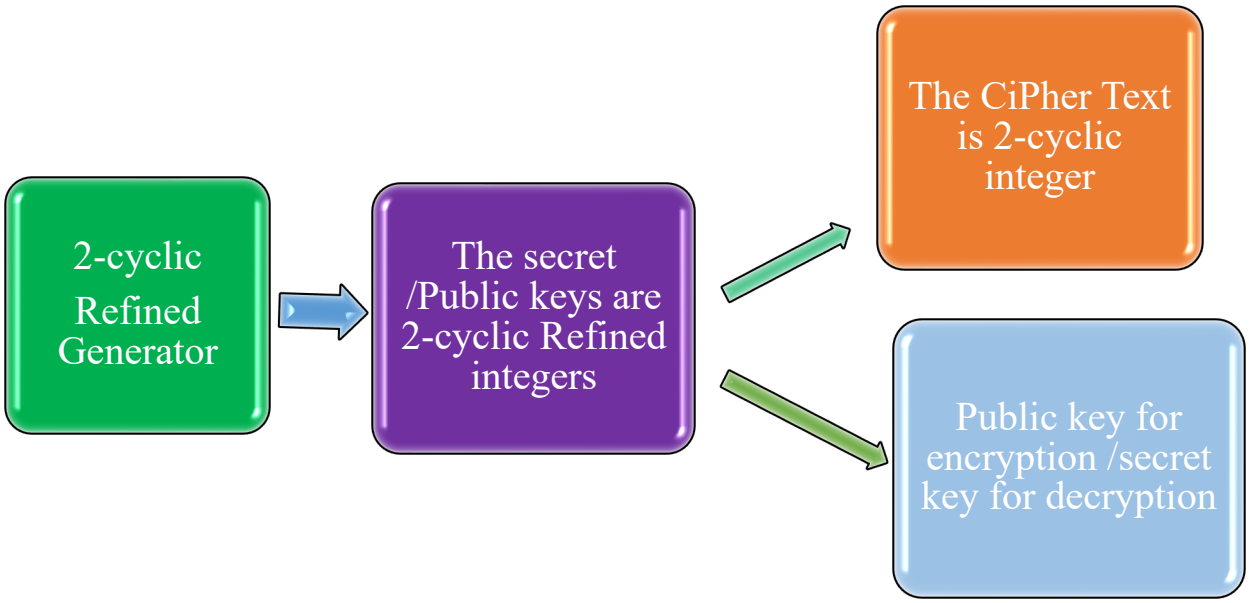

Figure 1 (a): description of 2-cyclic refined RSA algorithm

Doi : https://doi.org/10.54216/JCIM.120106
Received: December 24, 2022 Revised: February 15, 2023 Accepted: April 26, 2023

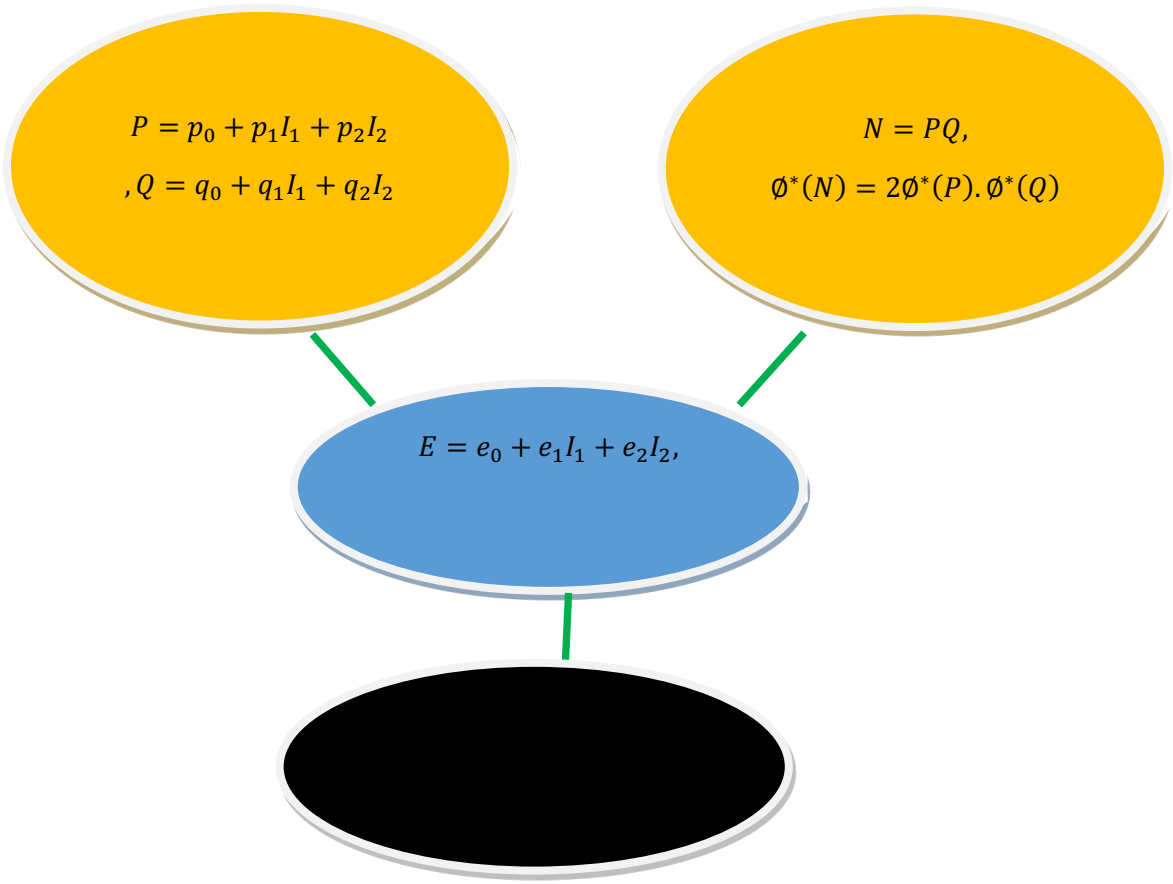

Figure 1 (b): description of 2-cyclic refined RSA algorithm

Example.
Suppose that (F) decides to send $M = 3 + 4I_1 + 2I_2$ to (E).
(E) picks $P = 13 + 2I_1 + 8I_2, Q = 7 + 4I_1$, $PQ = 91 + 52I_1 + 14I_1 + 18I_2 + 56I_2 + 32I_1 = 91 + 98I_1 + 64I_2$.
$\emptyset^*(N) = \frac{1}{2}\emptyset(13) \times \emptyset(23) \times \emptyset(19) \times \emptyset(7) \times \emptyset(11) \times \emptyset(3) = \frac{1}{2} \times 12 \times 22 \times 18 \times 6 \times 10 \times 2 = 285120.$
(E) picks $E = 7 + 3I_1 + 3I_2$ it is clear that:

$$\begin{cases} 0 < 7 < 285120, gcd(7,285120) = 1 \\ 0 < 7 + 3 + 3 = 13 < 285120, gcd(13,285120) = 1 \\ 0 < 7 - 3 + 3 = 7 < 285120, gcd(7,285120) = 1 \end{cases}$$

The public key is $(7 + 3I_1 + 3I_2, 91 + 98I_1 + 64I_2)$.
The encrypted message is:

$$M \equiv C^{E^{-1}} (mod\ N)$$
$$= 3^7 (mod\ 91) + \frac{1}{2} I_1 [9^{13} (mod\ 253) - 1^7 (mod\ 57)]$$
$$+ \frac{1}{2} I_1 [9^{13} (mod\ 253) + 1^7 (mod\ 57) - 2 \times 3^7 (mod\ 91)]$$
$$= 3 + \frac{1}{2} I_1 [269 - 1] + \frac{1}{2} I_1 [269 + 1 - 6] = 3 + 134 I_1 + 132 I_2$$

The second side (E) decrypts the message as follows:

Doi : https://doi.org/10.54216/JCIM.120106
Received: December 24, 2022 Revised: February 15, 2023 Accepted: April 26, 2023

$e_0{}^{-1}\left(mod\ \emptyset^*(N)\right) = 7^{-1}(mod\ 285120) = 81463$
$(e_0 + e_1 + e_2)^{-1}\left(mod\ \emptyset^*(N)\right) = 13^{-1}(mod\ 285120) = 65797$
$(e_0 - e_1 + e_2)^{-1}\left(mod\ \emptyset^*(N)\right) = 7^{-1}(mod\ 285120) = 81463$
The plain text is:
$M \equiv C^{E^{-1}}(mod\ N) = 3^{81463}(mod\ 91) + \frac{1}{2}I_1[16^{228725}(mod\ 253) - 1^{97129}(mod\ 57)] +$
$\frac{1}{2}I_1[16^{228725}(mod\ 253) + 1^{97129}(mod\ 57) - 2 \times 3^{81463}(mod\ 91)] = 3 + \frac{1}{2}I_1[9 - 1] + \frac{1}{2}I_1[9 + 1 - 6] = 3 + 4I_1 + 2I_2.$

4. Why should we use new algorithms?

In cryptography, it is important to maintain the confidentiality and the security, whether it is digital data, text, or even information of a military or medical nature. Therefore, we must use encryption systems with high efficiency and high complexity, as increased secrecy is closely related to the increased complexity of the algorithm and the difficulty of attacking it. Since the number system used in our new algorithm is three-dimensional, or in other words, described by three different components, this gives the process of exchanging keys or confidential data more security and reliability than using classical one-dimensional methods. It is possible that an attacker will be able to detect one of the components used but it will be very far from detecting the remaining two components that enter into the formation of the algebraic key structure.

The main difficulties facing these new algorithms are the following points:
1-) Until now, computers do not recognize these numerical systems because they are new, which presents a challenge for programmers to introduce them into programming languages so that it is easier for a computer to deal with them.
2-) Also, the use of these expanded numbers may result in a greater consumption of computer resources, which significantly affects the ability of the computer to deal with them within a useful and logical time.
These theses remain as challenges to the possible development of the theory of cryptography and its various applications in this time when the movement of interest in cyber-security and its applications is accelerating.

The diagram on the side shows that the time required to break the new algorithm is about three times the time required in the traditional algorithm, and sometimes slightly more, and this means that the new algorithm is three times superior to the traditional version in terms of efficiency and complexity.

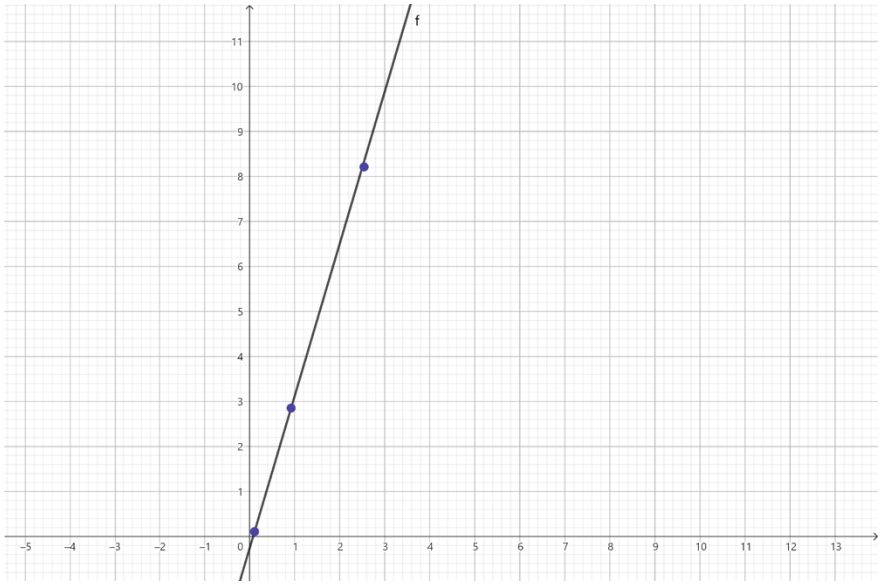

Figure 2: the performance of the new algorithm

Doi : https://doi.org/10.54216/JCIM.120106
Received: December 24, 2022 Revised: February 15, 2023 Accepted: April 26, 2023

Figure 3 shows a comparison between using integers and 2-cyclic refined integers in cryptography.

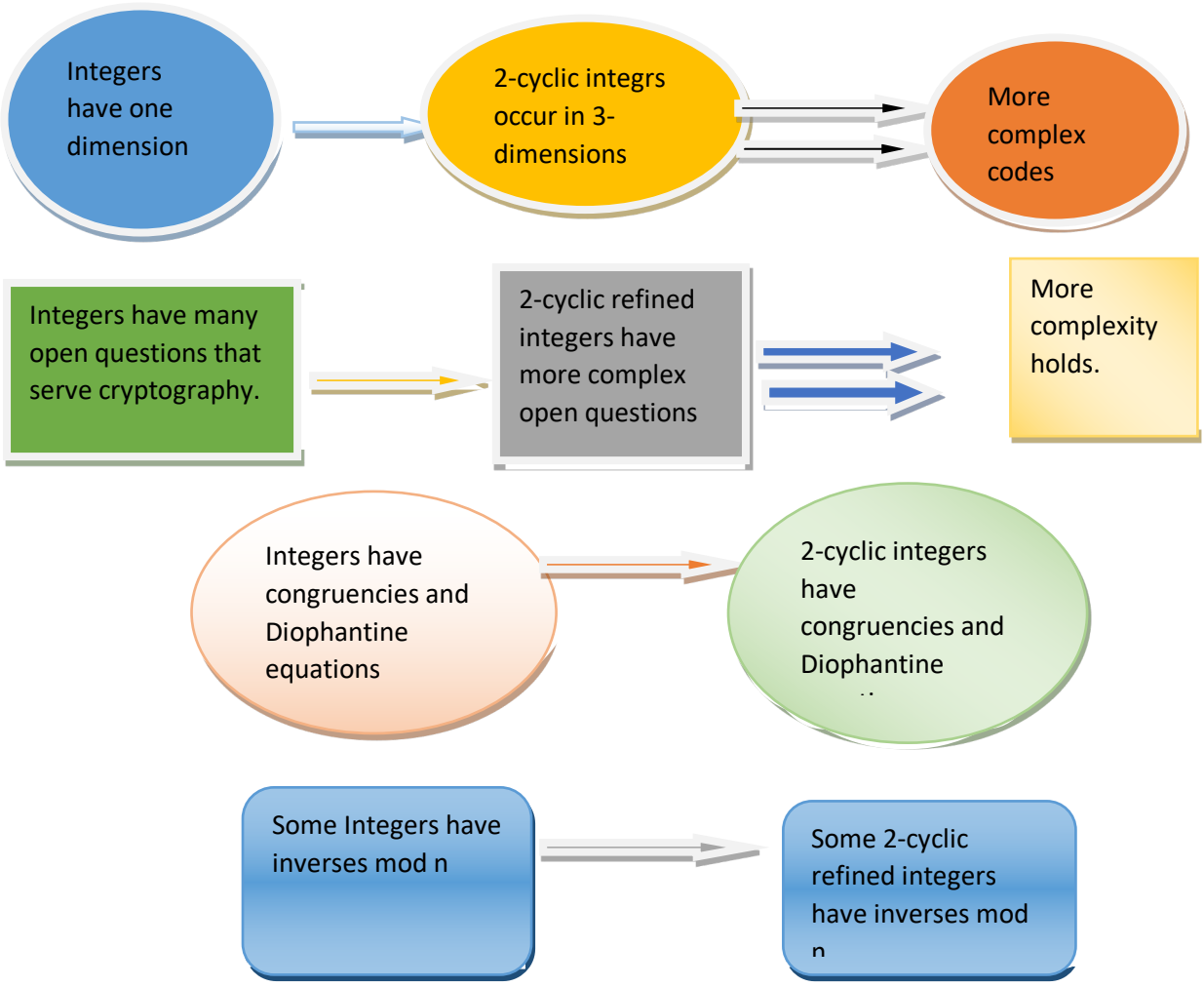

Figure 3: Comparison between using integers and 2-cyclic refined integers in cryptography.

5. Conclusion

In this paper, we have presented a novel algorithm for the encryption and the decryption of data and information based on RSA algorithm and the algebra of 2-cyclic refined integers. In addition, we have discussed the possible future applications of the novel algorithm with an example to clarify its validity. Also, many figures and tables were provided to explain the new algorithm with respect to the classical one.

References

[1] Abobala, M, "*n*-Cyclic Refined Neutrosophic Algebraic Systems Of Sub-Indeterminacies, An Application To Rings and Modules", International Journal of Neutrosophic Science, Vol. 12, pp. 81-95 . 2020.

[2] Sadiq. B., " A Contribution To The group Of Units Problem In Some 2-Cyclic Refined Neutrosophic Rings ", International Journal Of Neutrosophic Science, 2022.

[3] Von Shtawzen, O., " Conjectures For Invertible Diophantine Equations Of 3-Cyclic and 4-Cyclic Refined Integers", Journal Of Neutrosophic And Fuzzy Systems, Vol.3, 2022.

Doi : https://doi.org/10.54216/JCIM.120106
Received: December 24, 2022 Revised: February 15, 2023 Accepted: April 26, 2023

[4] Basheer, A., Ahmad, K., and Ali, R., " On Some Open Problems About n-Cyclic Refined Neutrosophic Rings and Number Theory", Journal Of Neutrosophic And Fuzzy Systems,, 2022

[5] Von Shtawzen, O., " On A Novel Group Derived From A Generalization Of Integer Exponents and Open Problems", Galoitica journal Of Mathematical Structures and Applications, Vol 1, 2022.

[6] Zayood, K., " On Novel Public-key Cryptosystem Using MDS Code", Neoma Journal Of Mathematics and Computer Science, 2023.
[7] Zayood, K., " On A Novel Generalization of The RSA Crypto-System", Neoma Journal Of Mathematics and Computer Science, 2023.
[8] Merkepci, M,; Sarkis, M. An Application of Pythagorean Circles in Cryptography and Some Ideas for Future Non Classical Systems. Galoitica Journal of Mathematical Structures and Applications **2022**.
[9] Abobala, M., and Allouf, A., " On A Novel Security Scheme for The Encryption and Decryption Of 2×2 Fuzzy Matrices with Rational Entries Based on The Algebra of Neutrosophic Integers and El-Gamal Crypto-System", Neutrosophic Sets and Systems, vol.54, 2023.
[10] Merkepci, M., Abobala, M., and Allouf, A., " The Applications of Fusion Neutrosophic Number Theory in Public Key Cryptography and the Improvement of RSA Algorithm ", Fusion: Practice and Applications, 2023.
[11] Merkepci, M., and Abobala, M., " Security Model for Encrypting Uncertain Rational Data Units Based on Refined Neutrosophic Integers Fusion and El Gamal Algorithm ", Fusion: Practice and Applications, 2023.
[12] Alhasan, Y., Alfahal, Aboubida., abdulfatah, R., Ali, R., and Aljibawi, M., " On A Novel Security Algorithm For The Encryption Of 3×3 Fuzzy Matrices With Rational Entries Based On The Symbolic 2-Plithogenic Integers And El-Gamal Algorithm", International Journal Of Neutrosophic Science, Vol.21, 2023.
[13] Al Basheer, O., " On Some Novel Simplex Linear Codes Defined Over The Algebraic Ring $\boldsymbol{F2+vF2}$ ", Neoma Journal Of Mathematics and Computer Science, 2023.

Doi : https://doi.org/10.54216/JCIM.120106
Received: December 24, 2022 Revised: February 15, 2023 Accepted: April 26, 2023