EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

Enhanced Security in Public Key Cryptography: A Novel Approach Combining Gaussian Graceful Labeling and NTRU Public Key Cryptosystem

S Kavitha[1,*], G Jayalalitha[2] and K Sivaranjani[3]

[1] VELS Institute of Science, Technology & Advanced Studies, Chennai, Tamilnadu, India
[2] Department of Mathematics, VELS Institute of Science, Technology & Advanced Studies, Chennai, Tamilnadu, India
[3] Sri Eshwar College of Engineering, Coimbatore, Tamilnadu, India

Abstract

This research explores an encryption system that combines the Nth-degree Truncated Polynomial Ring Unit (NTRU) public key cryptosystem with Gaussian Graceful Labeling. This process assigns distinct labels to a graph's vertices, resulting in successive Gaussian integers. The NTRU method offers enhanced security and efficient key exchange. The communication encryption process depends on integers P, a, and b, with P being the largest prime number in the vertex labeling. The original receivers are the vertex labeling with the largest prime number coefficient, while all other receivers receive messages from the sender. A polynomial algebraic mixing system and a clustering principle based on the abecedarian probability proposition are used in NTRU encryption and decryption. The choice of relatively prime integers p and q in NTRU plays a role in the construction of polynomial rings used for encryption and decryption, with specific choices and properties designed to ensure scheme security.

Keywords: Gaussian graceful labeling, NTRU public key cryptosystem, Security system, Encryption, Decryption

Received on 14 November 2023, accepted on 23 January 2023, published on 01 February 2024

doi: 10.4108/eetiot.4992

*Corresponding author. Email: kavithasundaram55@gmail.com

1. Introduction

The NTRU public key cryptosystem [1-3] and graceful labeling are two areas of research that have been extensively studied in isolation. However, there has been little research on the combined use of these two techniques. For the combined use of the NTRU public key cryptosystem and graceful labeling, this paper suggests fresh research avenues and creative applications. Increased computational complexity is one potential issue when using Graceful labeling in conjunction with the NTRU public key cryptosystem. Since both systems are known for having high computational demands, combining them could produce calculations that are even more difficult. The increased susceptibility to attacks is a potential disadvantage as well. Both systems are regarded as secure when used separately but combining them could introduce new weaknesses that attackers could use.

This research work discusses an effective encryption system that combines the Nth-degree truncated polynomial ring unit, shortened as the NTRU public key cryptosystem, with Gaussian Graceful Labeling. It is the process of assigning distinct labels to a graph's vertices from *0, z, 2z.... Pz* with Gaussian integers in such a way that the resulting edge labels are the successive Gaussian integers *z, 2z, 3z,... Pz.* The combination of the NTRU public key cryptosystem and graceful labeling has the potential to offer several benefits, including Enhanced Security and Efficient Key Exchange. The communication encryption process using the NTRU method depends on the integers P, a, and b. In Gaussian graceful labeling the vertices are labeled by 0,z,2z,….Pz.

In this research, P is taken from the coefficient of z in the vertex labeling and it should be the largest prime

number. Each vertex with labeling z to Pz denoted the receivers, and the vertex labeled by 0 denoted the sender, and a and b are the real and imaginary parts of the Gaussian integer z in the labeling process. In this process, the vertex labeling with the largest prime number coefficient are the original receivers; not all other receivers get any messages from the sender. A polynomial algebraic mixing system and a clustering principle based on the abecedarian probability proposition are both used in NTRU encryption and decryption. The choice of relatively prime integers p and q in NTRU plays a role in the construction of the polynomial rings used for encryption and decryption. The specific choices and properties of p and q are designed to ensure the security of the scheme.

1.1 Cryptography

Cryptography is the science and practice of secure communication. It includes strategies and procedures for protecting data from unlawful access while ensuring its confidentiality, integrity, authentication, and non-repudiation. In the past, cryptography has been essential for protecting the privacy of sensitive data and facilitating secure communication over insecure channels. Through cryptography, communication with outside parties protected. Authorised parties can only gain access to it by converting the information into an unreadable format with the proper key or password.

Since ancient times, people have used cryptography, with the earliest instances occurring in ancient Egypt. As it is used to protect receptive information in a variety of industries, including finance, healthcare, and government, it now plays a crucial part in modern security. Numerous fields use cryptography, such as secure communication (such as encrypted messaging and VPNs), digital signatures, secure data storage, and secure online transactions (such as using SSL or TLS for secure web connections). It is essential to remember that while cryptography offers a solid framework for secure communication, other elements, such as proper key handling, secure protocols, and vulnerability management, have a significant impact on how cryptography is implemented, how keys are managed, and how secure a system is overall. Cryptography keeps advancing and adapting to meet new challenges and threats to information security as technology advances.

1.2 NTRU Public Key Cryptosystem

Safe communication channels are crucial in the modern world, where data breaches and replicated attacks are on the rise. NTRU encryption is one such method that has gained recent popularity due to its efficiency and security. NTRU is a public key cryptosystem that offers secure encryption and digital signatures. The mathematical characteristics of polynomial rings and the complexity of particular lattice mathematics problems serve as the foundation for NTRU [4-6]. To create the encryption keys needed to protect sensitive data, NTRU is used. Due to its resistance to attacks from quantum computing and inability to be compromised using current computing technology, it is regarded as one of the most secure algorithms currently in use. In this work, we followed the notations of Clark et al and Benjamin et al.

Compared to other conventional techniques like RSA, encryption is a method for secure communication that shows promise [7]. It is quicker and more effective because it uses smaller key sizes. Its liability to specific attacks is one disadvantage, which should be taken into account when using it. For its computational competence and speed, NTRU provides faster computations and smaller key sizes for equivalent levels of security. The NTRU uses a public key for encryption and a private key for decryption, just like other public-key cryptosystems and these keys derived from truncated polynomial ring polynomials. While the public key was made available to the public, the private key was kept private.

NTRU is suitable for use in environments with limited resources, such as embedded systems or mobile devices, as it is quick and efficient in comparison to other public key encryption schemes. The NTRU algorithm can be seen as a lock-and-key system, for example. The private key functions like a key that can be used to unlock the message, whereas the public key is like a lock that can be used to secure communication. The NTRU algorithm, in contrast to conventional locks and keys, makes sure that only the intended receiver can unlock the communication by using sophisticated mathematical operations.

Comparing the NTRU Public Key System to other cryptographic solutions, there are several advantages. Its quickness is one of its main advantages. NTRU is much faster than other public key systems, which makes it perfect for use in massive applications like mobile and cloud computing. Additionally, NTRU requires less bandwidth and storage space than other systems due to its smaller key size. The resistance of NTRU to quantum attacks is another advantage. Quantum computers, which can easily compromise conventional public key systems, are not a factor in the NTRU system. This makes it a dependable choice for long-term safety requirements.

The IoT (Internet of Things) sector is where the NTRU system shows the most promise [8]. NTRU can be used to secure communication between various devices in IoT networks because it is compact and effective [9]. This is crucial because the computing and memory capabilities of these devices are frequently constrained, rendering conventional cryptographic systems useless. The financial sector is a further real-world application of the NTRU public key system [10]. The quick encryption and decryption times of NTRU make it perfect for protecting online financial transactions. In fact, NTRU is already being used for this purpose by a number of significant banks.

In conclusion, the NTRU cryptosystem offers an effective and secure method [11] for key exchange and public key encryption. In the face of evolving cryptographic challenges, NTRU offers a promising solution for secure communication by utilizing lattice-based mathematics and the effectiveness of polynomial operations.

Let (P,a,b) are three integers where $\gcd(a,b)=1, a<b$ and P is a prime integer. NTRU cryptosystem depends on the above three integers involved in the shortened polynomial ring of degree $P-1$ noted by $\Gamma = Z[Y]/(Y^P-1)$. Let $\Gamma_a = Z_a[Y]/(Y^P-1)$ and $\Gamma_b = Z_b[Y]/(Y^P-1)$ are the polynomial *mod a* and *mod b*.

The subset $\Omega_f, \Omega_g, \Omega_r, and\ \Omega_m$ defines as follows:

- The private keys selected from $\Omega_f = B(d_f)$.
- The other private keys selected from $\Omega_g = B(d_g)$.
- The polynomial set $m \in \Omega_m$ with co-efficient -1 *or* 0 *or* 1, that stand for encrypt messages and $\Omega_m = Z_a[Y]/(Y^P-1)$ is the plaintext space.
- $\Omega_r = B(d_r)$, used to select the blind value during the selection of encryption.

1.3 Conversion of Letters to Binary

Computers convert all messages, words, images, and other data into binary codes using some standard codes. This standardised system allows for seamless communication between different computer systems and ensures that information is transmitted accurately. ASCII has been in use since the early days of computing and remains an important part of modern technology. The computer then decodes this binary code to produce the desired output.

In 1960, ASCII become a universal standard for encoding characters. There are 128 characters total, which are made up of letters, numbers, punctuation, and control codes. The underlying principle is the same for the NTRU cryptosystem. Therefore, it is necessary to have a foundational understanding of this conversion. There are tables that can be used because this conversion is quite straightforward and always produces the same result. ASCII table given in the Appendix.

1.4 Gaussian Graceful Labeling

Graceful labeling techniques have been explored for applications in cryptography and data encryption. The unique labels assigned through graceful labeling can be used as encryption keys or components in cryptographic algorithms to secure data and communications. Kavitha et al. and Jayalalitha et al. defined the Gaussian Graceful labeling with Gaussian integers, offers several advantages and interesting properties. There are so many advantages to using Gaussian integers for graceful labeling. While using Gaussian integers in labeling, it increased the labeling flexibility. Gaussian integers provide a larger set of potential labels compared to the traditional use of positive integers in graceful labeling. This increased flexibility allows for more diverse and intricate labeling patterns, which can enhance the visual representation and understanding of complex graphs.

The use of Gaussian integers allows for the generation of labeling patterns that exhibit more complex and interesting structures. The presence of both real and imaginary parts in the labels can result in visually appealing and symmetrical patterns, enriching the visual representation of the graph. Gaussian integers naturally incorporate the concept of imaginary relationships through the imaginary component of the labels. This can be advantageous when dealing with graphs that represent systems with complex interactions or relationships that cannot be fully captured by simple integer labels. The use of Gaussian integers in graceful labeling connects the concept to number theory, specifically the study of complex numbers and their properties.

This connection can show the way to a deeper understanding of the mathematical aspects of graceful labeling and give opportunities for exploring new theoretical results and conjectures. Many real-world networks, such as societal networks, genetic networks, and communication networks, exhibit complex structures and interactions.

Graceful labeling with Gaussian integers can capture and represent these complex network properties more accurately, facilitating the analysis and study of such networks. The use of Gaussian integers in graceful labeling opens up new avenues for research and algorithmic exploration. Researchers can investigate the properties of Gaussian integer labeling, develop algorithms specific to this context, and explore the uniqueness and complexity aspects of graceful labeling with Gaussian integers.

The communication encryption process using the NTRU method depends on the integers P, a, and b. In Gaussian graceful labeling the vertices are labeled by 0,z,2z,….Pz. In this research, P is taken from the coefficient of z in the vertex labeling and it should be the largest prime number. Each vertex with labeling z to Pz denoted the receivers, and the vertex labeled by 0 denoted the sender, and a and b are the real and imaginary parts of the Gaussian integer z in the labeling process. In this process, the vertex labeling with the largest prime number coefficient are the original receivers; not all other receivers get any messages from the sender.

1.5 Benefits of Gaussian Graceful labeling with NTRU Method

One benefit of using graceful labeling with NTRU encryption is that it can help prevent attacks by ensuring that the labels are unique and difficult to guess. It is important to note that the use of Gaussian integers in graceful labeling may also introduce computational challenges due to the complex arithmetic operations involved. However, the advantages mentioned above make it an intriguing and valuable approach, particularly in contexts where the benefits of complex labeling patterns and relationships outweigh the computational complexities.

The NTRU public key cryptosystem is known for its strong security and resistance to attacks from quantum computers [12-14]. By combining it with graceful labeling,

which is used in graph theory to assign labels to vertices, an additional layer of security can be added to the system. The NTRU cryptosystem is also known for its efficiency in key exchange. By incorporating graceful labeling, which can be used to efficiently label vertices in a graph, the key exchange process can be further optimized.

Example of a Gaussian graceful labeling given in Fig 1 and Fig 2

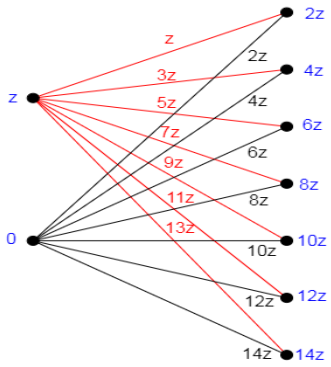

Figure 1 A Gaussian complete bipartite graph $K^{g}_{2,7}$

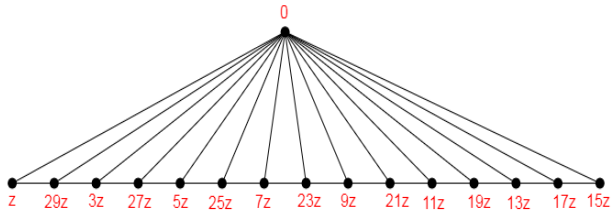

Figure 2 A Gaussian Fan graph $F^{g}_{1,15}$

The NTRU (Nth-degree Truncated Polynomial Ring) method and Gaussian graceful labeling are two distinct concepts that are not directly related.

The method involves generating keys based on polynomial coefficients and performing polynomial arithmetic operations for encryption and decryption. Gaussian Graceful labeling is a concept in graph theory, [15] as mentioned earlier, where distinct integers are assigned to the vertices of a graph such that the resulting vertex labels correspond to unique edge labels. It focuses on labeling vertices in a graph to facilitate various applications such as graph visualization, communication networks, error detection, and more.

While Gaussian graceful labeling and the NTRU method are both mathematical concepts [16], they belong to different areas of study. Gaussian Graceful labeling focuses on assigning labels to graph vertices, while the NTRU method is a cryptographic algorithm for secure communication and encryption. There is no direct relationship or application between the two. Here we relate both methods together.

2. Methods and Materials

2.1 Types of Components

Key Generation

NTRU generates two sets of polynomials during the key generation process: a public polynomial and a private polynomial. Encryption is performed using the public polynomial, while decryption is performed using the private polynomial. Random number generators and hash functions are employed to generate polynomials. Once the polynomials are generated, they are combined to form both keys [17]. The key generation process is crucial to ensuring secure communication because it determines the strength of the encryption. If the key is weak, attackers, compromising the security of the communication, can easily crack it [18]. Therefore, it is important to use a strong key generation process to ensure that the encryption is secure.

Encryption

The NTRU encryption algorithm involves, three main steps: key generation, encryption, and decryption. To generate a public and private key pair, NTRU uses a polynomial ring with coefficients in the integers modulo a prime number. The first key is derived from the second key using a process called the inverse Fourier transform. To encrypt a message, the sender multiplies the message by the recipient's public key and adds a random noise polynomial. The resulting cipher text is sent to the recipient, who can decrypt it using their private key.

Decryption

Decryption algorithms are similar in principle to encryption algorithms but reversed. The cipher text is multiplied by the private key polynomial f, resulting in a new polynomial g. Then, g is reduced modulo the public modulus polynomial a to obtain the plaintext polynomial m. The key to successful decryption lies in choosing the correct private key polynomial f. This requires knowledge of the factorization of the public modulus polynomial a. However, finding the factors of a, is a difficult problem that is believed to be computationally infeasible, making NTRU a secure encryption method.

The receiver can decrypt the received cipher text with the private key. The original message can be retrieved by applying specific mathematical operations to the encrypted polynomial with the private key.

Digital Signatures

NTRU can also be used for generating digital signature, given that authenticity and integrity to messages. The signer generates a polynomial signature using their private key. The receiver can confirm the signature's authenticity by applying mathematical operations by the signer's public key.

2.2 Proposed Method

In order to improve security and safeguard sender and receiver's private data, this research suggests employing real and imaginary parts of integers as system parameters for the NTRU approach. Investigate the combined system's security, pinpoint any weaknesses, and create new, more effective and secure algorithms for fusing the NTRU public key cryptosystem with graceful labelling [19]. Examine how the two systems can work together in areas like authentication, data encryption, and secure communication.

Gaussian graceful labeling effectively protects the sender and receiver's secrets, which labels vertices and edges using real and imaginary integers. This strategy guarantees effective sensitive information protection in the NTRU method. The NTRU approach can boost security by using the real and imaginary parts of integers as system parameters. This is because the combination of these settings raises the amount of complexity of the encryption technique, making it more difficult for potential attackers to decode the sensitive data. Additionally, by incorporating Gaussian graceful labeling into this approach, the protection of sender and receiver's secrets is further strengthened, guaranteeing a robust safeguard for sensitive data [20].

2.3 Processing of Efficient Encryption Method

Step 1

Binary and Polynomial Conversion

Bring into play the American Standard Code for Information Interchange, or ASCII, (https://www.ascii-code.com/) to transform all messages, words, images, and other data into binary codes and then to polynomials.

Step 2

Choose parameters

Select parameters for the NTRU scheme, such as the degree of polynomials, the modulus, and other system parameters. Choose P,a,b

Here we choose $a,basz=a+ib$ in Gaussian graceful labeling and also $\gcd(a,b)=1$ and $b>a$.

Step 3

Key Generation

- Generate a private key by randomly selecting polynomials f and g of a specified degree with coefficients in a finite ring.
- Compute f_a *and* f_b
- Compute $h \equiv g * f_b \,(\mathrm{mod}\, b)$.
- Publish the set of parameters $a,b,\Omega_f,\Omega_g,\Omega_r$ *and* Ω_m and also publish the public key (P,h) .
- Maintain the secret key (f, f_a) .

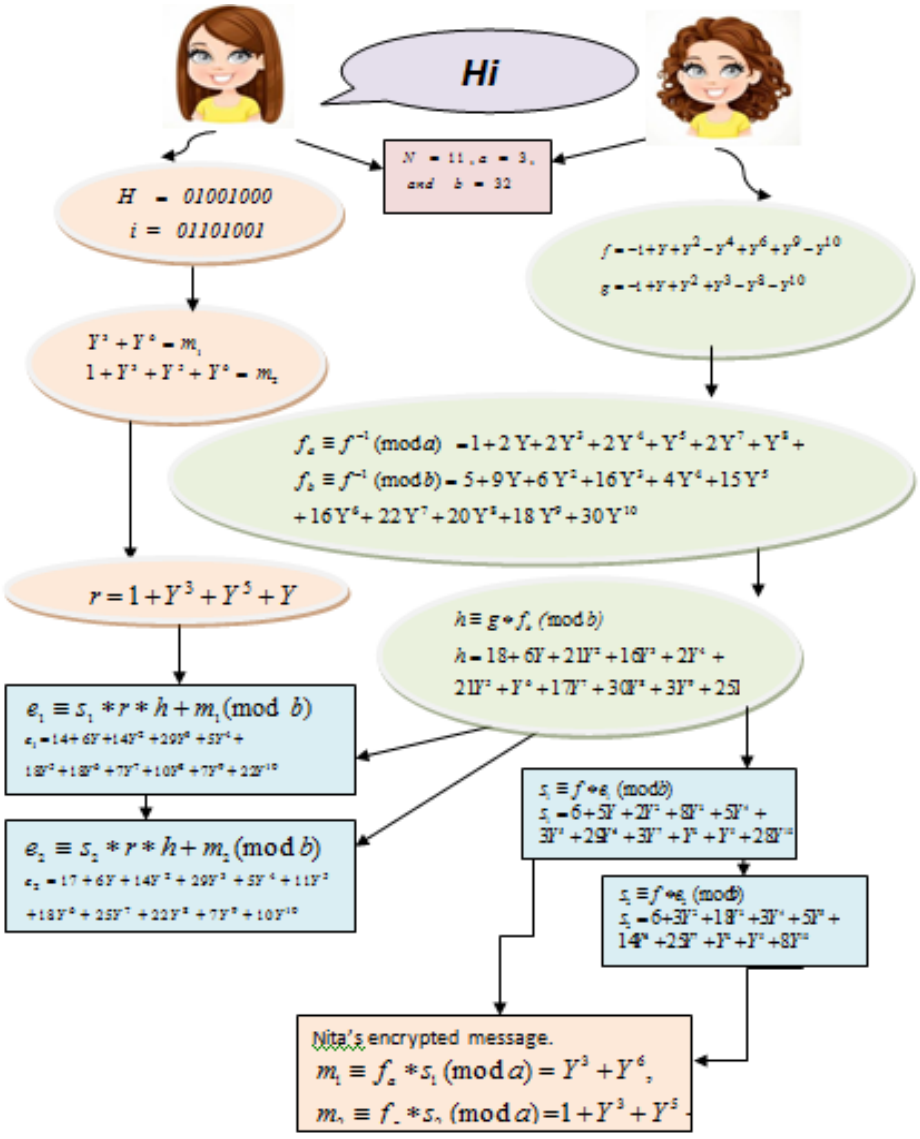

Figure 3. Process of NTRU Encryption

3. Conclusion

To sum up, the NTRU encrypted method and graceful labeling have proven to be effective tools for data security and cryptography. Writing a conclusion for this approach was crucial, though, as it aids readers in understanding its advantages and disadvantages as well as how it might improve in subsequent studies. Even though NTRU and graceful labeling were two separate ideas, they could have been combined in some situations. A graph's vertices, for instance, could be labeled using graceful labeling before being encrypted with NTRU. This can offer a safe method of sending delicate data over a network. This may result in more development in the area, which would ultimately help society as a whole. The NTRU method's fundamental components were (P, a, and b), and the Gaussian graceful labelings fundamental components are the coefficient numbered and the Gaussian integer z, which included real and imaginary parts. Therefore, the NTRU method was appropriate for this research.

Exploring the possibility of used quantum computing to defeat NTRU encryption and Gaussian graceful labelling could be one area of future researched. These encryption techniques might become less reliable as quantum computing developed. Future research may focus significantly on examined potential weaknesses in these techniques and figuring out how to make them more resistant to quantum attacked. Future studied could also examined how NTRU encryption and Gaussian graceful labelling might be combined with other encryption techniques to produced systems that are even more secure.

It might be possible to build a system that is more difficult to cracked and resistant to a wider variety of attacked by combining several techniques. Future research could be interested in examining how these techniques might be used in various contexts, such as cloud computing or IoT devices.

Appendix A.

The downloads of ASCII letters to binary from https://www.ascii-code.com

A	01000001	a	01100001
B	01000010	b	01100010
C	01000011	c	01100011
D	01000100	d	01100100
E	01000101	e	01100101
F	01000110	f	01100110
G	01000111	g	01100111
H	01001000	h	01101000
I	01001001	i	01101001
J	01001010	j	01101010
K	01001011	k	01101011
L	01001100	l	01101100
M	01001101	m	01101101
N	01001110	n	01101110
O	01001111	o	01101111
P	01010000	p	01110000
Q	01010001	q	01110001
R	01010010	r	01110010
S	01010011	s	01110011
T	01010100	t	01110100
U	01010101	u	01110101
V	01010110	v	01110110
W	01010111	w	01110111
X	01011000	x	01111000
Y	01011001	y	01111001
Z	01011010	z	01111010

References

[1] Seidel T, Socek D. Parallel Symmetric Attack on NTRU using Non-Deterministic Lattice Reduction. Designs, Codes and Cryptography.2004; Vol.32: p. 369-379.

[2] Fujisaki E. Okamoto T How to Enhance the Security of Public-Key Encryption at Minimum Cost, In: PKC '99, of LNCS, Springer-Verlag. Vol. 1560 :1999. p. 53–68

[3] Clark, Benjamin. Understanding the NTRU Cryptosystem Williams Honors College, Honors Research Projects.906 2019;Vol.78: p. 96-112.

[4] An S, Kim S, Jin S, Kim H, Kim H. Single Trace Side Channel Analysis on NTRU Implementation. Applied Sciences. 2018; Vol.8(11):2014.

[5] Nitaj A. The Mathematics of the NTRU Public Key Cryptosystem. Addepalli VN Krishna (Eds.). Emerging Security Solutions Using Public and Private Key Cryptography: Mathematical Concepts, IGI Global, 2015.

[6] Hoffstein J, Pipher J, Silverman JH. NTRU: A ring-based public key cryptosystem. In: Buhler, J.P. (eds) Algorithmic Number Theory. ANTS 1998. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg: 1998. Vol.1423:p. 267–288

[7] Koblitz N. Elliptic curve cryptosystems, Mathematics of Computation Journal.1987; Vol.48: p. 203–209 .

[8] Bambang Harjito, Henny Nurcahyaning Tyas, Esti Suryani, Dewi Wisnu Wardani. Comparative Analysis of RSA and NTRU Algorithms and Implementation in the Cloud. IJACSA.2022; Vol.13[3]: p. 13-25.

[9] Stallings W. Cryptography and Network security: Principles and Practice. 4th Edition. Boston: Pearson Education; 2017. Vol.1: p. 582-596.

[10] Sarah Hussain Shahhadi, Hassan Rashed Yassein. A New Design of NTRU Encrypt-analog Cryptosystem with High Security and Performance Level via Tripternion Algebra, IJMCS. 2021; Vol. 4: p. 1515–1522.

[11] Diffie W, Hellman M. New directions in cryptography. IEEE.Trans. Inf.Theor. 1976; Vol.22: p. 644-654.

[12] Ustimenko VA. Graphs with special arcs and cryptography. Acta Appl. Math. 2002; Vol.74: p. 117-153.

[13] Coglianese M. MaTRU:A New NTRU- Based Cryptosystem. Progress in Cryptology - Lecture Notes in Computer Science. 2005.Vol. 3797: p. 232-243.

[14] Jaulmes E, Joux A. A chosen-cipher attack against NTRU. Lecture Notes in Computer Science.2000. Vol.1880: p.20–35.

[15] Laarhoven T, Van de Pol J. Solving hard lattice problems and the security of lattice-based cryptosystems. Cryptology ePrint Archive. 2012.Vol.2012: p. 533-576.

[16] Coppersmith D, Shamir A. Lattice attacks on NTRU. In: Advances in cryptology, EUROCRYPT'97, Lecture Notes in Computer Science. Berlin. Springer;1997. Vol. 1233: p. 52–61.

[17] El Gamal T. A public key cryptosystem and signature scheme based on discrete logarithms. IEEE Transactions on Information Theory. 1985.Vol.31: p. 469–472.

[18] Pushpalatha N, Prasanth A. Enterprise Data. Data Fabric Architectures: Web-Driven Applications.2023. Vol. 36, p. 95-114.

[19] Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM 21.1978.p. 120-126.

[20] Coppersmith D, The Data Encryption Standard (DES) and its strength against attacks. IBM Journal of Research and Development. May 1994. Vol. 38[3]: p. 243-250.