A COMPUTATIONALLY EFFICIENT APPROACH TO THE ROLE OF NUMBER THEORY IN CRYPTOGRAPHY

[1]Mimanshi Giri and [2]Dr. Ankur Nehra
[1]M.Sc (Mathematics) 1st Sem., Department of Mathematics, Dhanauri P.G. College, Haridwar, Uttarakhand, 24766, India
[2]Supervisor, Department of Mathematics, Faculty of Science, Dhanauri P.G. College, Haridwar, Uttarakhand, 24766, India, [2]drankurnehra123@gmail.com
Corresponding Author: [1]mimanshigiri0008@gmail.com

Abstract: Number theory plays a crucial role in modern cryptography by providing the mathematical foundation for secure communication systems. Concepts such as prime numbers, modular arithmetic, and number-theoretic functions are central to the design of encryption and decryption algorithms. Many widely used cryptographic methods, including RSA, Diffie-Hellman key exchange, and elliptic curve cryptography, rely on the computational difficulty of solving certain number-theoretic problems. This paper examines how number theory underpins cryptographic techniques, explores its applications in securing digital information, and discusses emerging challenges such as quantum computing. Understanding the role of number theory highlights its importance in ensuring data confidentiality, integrity, and authentication in the digital age.

[Giri, M. and Nehra, A. **A COMPUTATIONALLY EFFICIENT APPROACH TO THE ROLE OF NUMBER THEORY IN CRYPTOGRAPHY**. *The International Journal of Interpretation, Observation and Analysis*, 2026; Volume 1, Issue 1 (January-March): Page Number: 13-20. **ISSN 2349-0713, Peer-reviewed (online/offline), Refereed, Indexed and International Journal (Since 2013), Global Impact Factor: 6.489**

Keywords: Number Theory, Cryptographic Algorithms, Computational Efficiency, Public Key Cryptography, Mathematical Security

INTRODUCTION

In the modern digital era, the protection of information has become a fundamental necessity. Cryptography serves as the primary tool for securing data transmitted across open networks, and its effectiveness relies heavily on mathematical principles, particularly number theory. Concepts such as prime numbers, modular arithmetic, and computational hardness form the foundation of many encryption and authentication techniques. This paper introduces the role of number theory in cryptography by exploring how these mathematical ideas are applied in widely used cryptographic algorithms. By examining their significance and applications, the study highlights the importance of number theory in ensuring secure and reliable communication systems. In the digital age, the protection of information has become one of the most critical challenges. Every time we send a message, make an online payment, or access secure data, cryptography ensures that our communication remains private and protected from unauthorized users. Cryptography is the science and art of securing information through mathematical techniques. Among the various mathematical branches supporting cryptography, number theory plays a central and indispensable role. Number theory, often called the "Queen of Mathematics", deals with the properties and relationships of integers. Though once regarded as purely theoretical, number theory today forms the mathematical foundation of many cryptographic algorithms. Its concepts, such as prime numbers, modular arithmetic, Euler's theorem, Fermat's little theorem, and Chinese Remainder Theorem, are essential for creating secure encryption systems that protect modern communication networks. Historically, cryptography was limited to simple substitution and transposition ciphers used by ancient civilizations. However, the growth of digital technology and electronic communication in the 20th and 21st centuries demanded stronger and more complex encryption methods. The shift from classical to modern cryptography brought mathematics, especially number theory, to the forefront. Algorithms such as the RSA (Rivest-Shamir-Adleman) encryption, Diffie-Hellman key exchange, and Elliptic Curve Cryptography (ECC) are all built upon number-theoretic principles. The security of these algorithms depends on mathematical problems that are easy to perform in one direction but extremely difficult to reverse, such as factoring large composite numbers or computing discrete logarithms.

LITERATURE REVIEW

Elliptic Curve Cryptography (ECC) has emerged as one of the most efficient public-key cryptographic paradigms due to its ability to provide strong security with smaller key sizes compared to traditional cryptosystems. The foundational works by Miller

Paper received: 14.12.2025 Reviewed: 20.12.2025 Accepted: 28.12.2025 Published: 02.01.2026

(1986) and Koblitz (1987) established the theoretical and practical framework of ECC, highlighting its applicability in secure communications. Subsequently, Edwards (2007) introduced a new normal form for elliptic curves, which significantly improved the efficiency of elliptic curve operations. Bernstein et al. (2007, 2008) further enhanced this model by proposing twisted Edwards curves, offering faster point addition and doubling operations with unified formulas, thereby reducing vulnerability to side-channel attacks. Research during the 2010s focused extensively on alternative curve representations and performance optimization. Studies by Ashraf and Kirlar (2012), Moody (2010), and Bianco and Gorla (2016) explored generalized, twisted, and trace-zero Edwards curve models, emphasizing compression techniques and computational benefits. Parallelly, works such as Dugardin et al. (2017) and Fournaris et al. (2019) addressed implementation security, proposing countermeasures against fault and side-channel attacks in Edwards curve-based cryptosystems. With the increasing demand for high-performance cryptographic systems, researchers began exploring mathematical optimization techniques. Vedic Mathematics, rooted in ancient Indian computational methods, gained attention for its potential to reduce arithmetic complexity. The seminal text by Bharati Krishna Tirthaji (1965) laid the foundation for Vedic arithmetic techniques, which were later adapted for modern digital computation. From 2018 onwards, significant contributions were made by Kumar, Nehra, Gupta, and their collaborators, who systematically integrated Vedic Mathematics techniques into ECC. Manoj Kumar and Ankur Kumar (2019-2020) presented a series of studies applying Vedic sutras to ECC over various curve forms, including Jacobian, Hessian, Huff, twisted Huff, Edwards, and twisted Edwards curves. Their works demonstrated notable improvements in point addition, doubling, tripling, and scalar multiplication operations by reducing computational overhead. The use of Advanced Indian Vedic Mathematics (AIVM) techniques further enhanced execution speed and resource efficiency. Karthikeyan and Jagadeeswari (2020) validated these findings by implementing low-power, high-speed Vedic multipliers for ECC, highlighting the suitability of such techniques for resource-constrained environments. Kumar and Gupta (2020) extended this research to Weierstrass curves, confirming the adaptability of Vedic Mathematics across different ECC representations. Literature surveys by Manoj Kumar and Ankur Kumar (2019) consolidated these developments, identifying Vedic Mathematics as a promising optimization approach for cryptographic arithmetic. Simultaneously, advancements in secure communication protocols were reported. Nehra and Man (2022) proposed a Chebyshev chaotic map-based authenticated key agreement scheme, reinforcing the role of ECC in satellite and vehicular communications. Kumar, Gupta, and Kumar (2024) analyzed fog-computing-based vehicular communication systems, emphasizing the necessity of computationally efficient cryptographic primitives in emerging network architectures. Recent studies (2018-2024) also explored post-quantum and isogeny-based cryptographic schemes using Edwards curves. Azarderakhsh et al. (2018) introduced EdSIDH, leveraging supersingular isogenies on Edwards curves, while Kim et al. (2019) proposed optimized methods for computing odd-degree isogenies. These works underscore the continued relevance of Edwards curves in next-generation cryptography. By 2025, the literature clearly indicates a convergence of three major research directions: (i) efficient elliptic curve models such as Edwards and twisted Edwards curves, (ii) arithmetic optimization using Vedic Mathematics techniques, and (iii) secure and scalable cryptographic applications in modern communication systems. Despite substantial progress, there remains scope for developing unified frameworks that systematically integrate Vedic Mathematics into modern cryptographic systems while balancing efficiency, security, and implementation feasibility.

NUMBER THEORY IN CRYPTOGRAPHY

Number theory provides the core mathematical principles used to design secure and efficient cryptographic algorithms. It focuses on concepts such as prime numbers, divisibility, modular arithmetic, congruences, and number-theoretic functions, which are essential for encryption and decryption processes. Cryptographic techniques like RSA, Diffie-Hellman key exchange, Elliptic Curve Cryptography (ECC), and Digital Signatures rely heavily on number theory. Key number-theoretic problems, such as integer factorization, the discrete logarithm problem, and the elliptic curve discrete logarithm problem, are computationally hard to solve, making them ideal for ensuring data security. At the same time, number theory enables efficient computation for legitimate users through optimized algorithms, modular exponentiation, and arithmetic over finite fields. Thus, number theory plays a crucial role in balancing computational efficiency and security, making it indispensable in the development of modern cryptographic systems.

Paper received: 14.12.2025 Reviewed: 20.12.2025 Accepted: 28.12.2025 Published: 02.01.2026

COMPUTATIONAL EFFICIENCY

Computational efficiency refers to the ability of cryptographic algorithms based on number theory to perform mathematical operations such as modular arithmetic, prime factorization, and exponentiation using minimal computational resources. It focuses on reducing time complexity, memory usage, and processing overhead while maintaining strong security guarantees. Efficient number-theoretic techniques enable faster encryption and decryption, lower energy consumption, and improved performance in real-time and resource-constrained environments such as IoT devices, embedded systems, and mobile platforms. Thus, computational efficiency plays a crucial role in designing practical and scalable cryptographic systems.

MATHEMATICAL SECURITY

Mathematical security in cryptography refers to the protection of cryptographic systems based on the inherent computational hardness of well-defined mathematical problems, particularly those derived from number theory. In this approach, security is not dependent on the secrecy of the algorithm but on the infeasibility of solving certain mathematical problems within a reasonable time using existing computational resources. In number-theoretic cryptography, mathematical security relies on problems such as large integer factorization, discrete logarithm problems, elliptic curve discrete logarithms, and modular arithmetic operations. These problems are considered computationally hard, meaning that no efficient polynomial-time algorithms are known to solve them for sufficiently large parameters. A computationally efficient cryptographic approach balances strong mathematical security with optimized arithmetic operations, ensuring high performance without compromising security. Efficient algorithms for modular exponentiation, prime number generation, and arithmetic over finite fields enhance system performance while preserving resistance against brute-force and cryptanalytic attacks. Thus, mathematical security ensures that even if an adversary has full knowledge of the cryptographic algorithm, breaking the system remains practically impossible due to the underlying complexity of number-theoretic problems.

PUBLIC KEY CRYPTOGRAPHY

Public Key Cryptography, also known as asymmetric cryptography, is a cryptographic technique that uses a pair of mathematically related keys: a public key and a private key. The public key is openly distributed and used for encryption or signature verification, while the private key is kept secret and used for decryption or digital signing. The security of public key cryptography relies heavily on number-theoretic problems that are computationally efficient to perform in one direction but infeasible to reverse without the private key. Core cryptographic systems such as RSA, Diffie-Hellman key exchange, and Elliptic Curve Cryptography (ECC) are built upon fundamental concepts of number theory, including prime factorization, modular arithmetic, discrete logarithms, and elliptic curve algebra. For example, RSA security depends on the difficulty of factoring large composite numbers, whereas ECC relies on the hardness of the elliptic curve discrete logarithm problem. Public key cryptography enables secure communication over insecure networks without requiring a pre-shared secret. It provides essential security services such as confidentiality, authentication, key exchange, and digital signatures. Due to ongoing research in computational efficiency, modern public key schemes increasingly focus on optimizing arithmetic operations and reducing key sizes while maintaining strong security, making them suitable for resource-constrained environments such as IoT and cloud-based systems.

CRYPTOGRAPHIC SYSTEMS

Cryptography is a fundamental discipline of information security that focuses on protecting data from unauthorized access and malicious attacks during storage and transmission. It employs mathematical algorithms and techniques to transform sensitive information into an unreadable format, ensuring confidentiality, integrity, authentication, and non-repudiation. With the rapid growth of digital communication, cloud computing, and Internet-based services, cryptography has become essential for securing data in modern information systems. Modern cryptographic systems rely on complex mathematical operations such as large integer arithmetic, modular exponentiation, and elliptic curve computations. These operations form the core of widely used cryptographic schemes, including symmetric-key algorithms, asymmetric-key algorithms, and cryptographic hash functions. While these methods provide strong security, they often require significant computational resources, which can impact performance, especially in resource-constrained environments such as embedded systems and Internet of Things (IoT) devices. As the demand for high-speed and energy-efficient security solutions increases, researchers are exploring alternative mathematical approaches to optimize cryptographic computations. In this context, Vedic Mathematics has emerged as a promising technique for enhancing computational efficiency. By integrating efficient

Paper received: 14.12.2025 Reviewed: 20.12.2025 Accepted: 28.12.2025 Published: 02.01.2026

arithmetic strategies from Vedic Mathematics into cryptographic algorithms, it is possible to reduce computational complexity while maintaining robust security. This research focuses on understanding cryptography and exploring innovative mathematical techniques to improve the performance of modern cryptographic systems.

OVERVIEW OF NUMBER THEORY

Number theory is a branch of mathematics that deals with the study of integers and their properties. Often referred to as pure mathematics, number theory focuses on patterns, relationships, and structures within whole numbers. Despite its theoretical origins, number theory has become a cornerstone of modern cryptography due to its applicability in secure communication systems. One of the most important concepts in number theory is prime numbers. Prime numbers are integers greater than one that have no positive divisors other than one and themselves. Their unique factorization properties make them essential in cryptographic algorithms, particularly in public-key encryption schemes. Another fundamental concept is divisibility, which examines how integers divide one another. Closely related to this is the greatest common divisor (GCD), a concept used to determine whether two numbers are relatively prime. The Euclidean algorithm, a number-theoretic method for computing the GCD, is widely used in cryptographic computations. Modular arithmetic is another key area of number theory. It involves arithmetic operations performed under a fixed modulus and is often described as "clock arithmetic." Modular arithmetic enables efficient encryption and decryption processes and is central to many cryptographic protocols. Number theory also includes important functions such as Euler's Totient Function, which counts the number of integers less than a given number that are relatively prime to it. This function plays a crucial role in the mathematical foundations of encryption algorithms like RSA. Overall, number theory provides the mathematical framework that makes cryptography both practical and secure. Its concepts allow for the creation of algorithms that are computationally efficient to execute but extremely difficult to break, making it indispensable in the field of information security. Number theory is one of the oldest and most fascinating branches of mathematics. It is primarily concerned with the study of integers and their properties. Initially, number theory was considered a purely theoretical subject with little practical application. However, with the advent of digital technology, it became a powerful tool in modern cryptography. The ability to protect digital information depends on mathematical operations that are easy to compute but hard to reverse, a property that naturally arises from number theory. This chapter provides an overview of the fundamental concepts of number theory that form the foundation of cryptographic systems.

CRYPTOGRAPHIC ALGORITHMS

Cryptographic algorithms form the core of secure communication systems by employing mathematical and number-theoretic principles to protect data confidentiality, integrity, and authenticity. In this study, the focus is on computationally efficient cryptographic algorithms that are strongly rooted in number theory.

Symmetric Key Algorithms

Symmetric cryptographic algorithms use a single secret key for both encryption and decryption. Although they are computationally fast, their security relies on secure key distribution rather than number theory. Examples include:

Asymmetric

Asymmetric cryptography heavily depends on number theory and forms the primary focus of this work. These algorithms use a pair of keys public and private and derive their security from complex mathematical problems such as integer factorization and discrete logarithms. Key algorithms include:

- RSA (Rivest-Shamir-Adleman): Based on the difficulty of factoring large prime numbers.
- Diffie-Hellman Key Exchange: Relies on the discrete logarithm problem.

Elliptic Curve Cryptography (ECC): Uses algebraic structures of elliptic curves over finite fields to provide high security with smaller key sizes and improved computational efficiency.

Hash Functions

Cryptographic hash functions use number-theoretic concepts to generate fixed-length outputs from arbitrary input data. They are widely used for data integrity and authentication. Common examples include:

- SHA-256
- SHA-3

Digital Signature Algorithms

Digital signatures ensure message authenticity and non-repudiation using number-theoretic foundations. Examples include:

- RSA Digital Signature Algorithm
- Digital Signature Algorithm (DSA)
- Elliptic Curve Digital Signature Algorithm (ECDSA)

Overall, number theory-based cryptographic algorithms provide strong security guarantees while

Paper received: 14.12.2025 Reviewed: 20.12.2025 Accepted: 28.12.2025 Published: 02.01.2026

maintaining computational efficiency, making them suitable for modern applications such as secure communication, cloud security, and blockchain systems.

ROLE OF NUMBER THEORY IN CLASSICAL CRYPTOGRAPHIC ALGORITHMS

Classical cryptographic algorithms, developed before the widespread use of computers, relied on simple mathematical principles to conceal information. Although these methods were less complex than modern cryptographic systems, number theory still played an important role in their design and operation. Concepts such as modular arithmetic, arithmetic operations on integers, and frequency properties of numbers formed the basis of many classical ciphers. One of the earliest examples is the Caesar cipher, which uses a fixed shift of letters in the alphabet. This cipher can be represented mathematically using modular arithmetic, where each letter is assigned a numerical value and encryption is performed using addition modulo 26. Despite its simplicity, this demonstrates how modular arithmetic underpins even the most basic encryption techniques. The Vigenère cipher, a polyalphabetic substitution cipher, also relies on modular arithmetic. Each letter of the plaintext is shifted by a value determined by a repeating keyword, with calculations performed modulo 26. While more secure than simple substitution ciphers, it is still vulnerable to frequency analysis. Transposition ciphers, which rearrange the positions of characters rather than substituting them, use permutation concepts closely related to number theory and combinatorics. The security of these ciphers depends on the number of possible arrangements, which is determined by mathematical counting principles. Although classical cryptographic algorithms are no longer secure against modern attacks, they played a significant role in the development of cryptography. They introduced fundamental number-theoretic concepts that later evolved into the sophisticated mathematical frameworks used in modern cryptographic systems.

ROLE OF NUMBER THEORY IN MODERN CRYPTOGRAPHY

Modern cryptography depends heavily on complex number-theoretic problems that are easy to compute but difficult to reverse.

RSA Algorithm

RSA is a public-key encryption system based on the difficulty of factoring large composite numbers into prime factors. It uses modular exponentiation and Euler's Totient Function to generate secure encryption and decryption keys.

Diffie-Hellman Key Exchange

The Diffie-Hellman protocol allows secure key exchange over a public channel. It relies on modular arithmetic and the difficulty of solving discrete logarithm problems.

Elliptic Curve Cryptography (ECC)

ECC uses algebraic structures from number theory and provides strong security with smaller key sizes. It is widely used in mobile devices and secure internet communication.

CONCLUSION

Number theory plays a fundamental and indispensable role in the field of cryptography. Mathematical concepts such as prime numbers, modular arithmetic, and number-theoretic functions provide the foundation for both classical and modern cryptographic algorithms. These principles enable the creation of secure encryption techniques that protect sensitive information from unauthorized access. From early substitution ciphers to advanced public-key systems like RSA and elliptic curve cryptography, number theory has continuously shaped the development of secure communication methods. Its ability to produce problems that are easy to compute but difficult to reverse ensures the strength and reliability of cryptographic systems. As digital communication continues to expand and new technologies such as quantum computing emerge, the importance of number theory in cryptography will only increase. Ongoing research in number theory will be essential for developing future cryptographic solutions that can meet evolving security challenges and safeguard information in the digital age.

REFERENCES

1. Ankur Kumar, Pratik Gupta, and Manoj Kumar, "Performance Analysis of a Fog-Computing-Based Vehicular Communication," International Journal of Vehicle Information and Communication Systems, Journal: International Journal of Vehicle Information and Communication Systems (IJVICS), Volume 9, Issue 2, Pages 115-134, 2024
2. Ankur Kumar, Pratik Gupta, Manoj Kumar, "Techniques of Vedic Mathematics for ECC over Weierstrass Curves," Advances in Communication and Computational Technology, Vol. 668, pp. 501-515, 2020.
3. Ankur Nehra, Dharminder Man, "A Construction of Chebyshev Chaotic Map-Based Authenticated Key Agreement for

Paper received: 14.12.2025 Reviewed: 20.12.2025 Accepted: 28.12.2025 Published: 02.01.2026

Satellite Communication," Security and Privacy, Vol. 5, Issue 6, 2022.

4. Ankur Nehra, Pratik Gupta, "Efficient Point Tripling Algorithms for Elliptic Curves using Vedic Mathematics," International Transactions in Mathematical Sciences and Computers,
Vol. 14, Issue 2, pp. 79-93, 2021.
5. Ashraf M., Kirlar B. B., "On the Alternate Models of Elliptic Curves," International Journal of Information Security Science, Vol. 1, Issue 2, pp. 49-66, 2012.
6. Azarderakhsh R., Lang E. B., Jao D., Koziel B., "EdSIDH: Supersingular Isogeny Diffie-Hellman Key Exchange on Edwards Curves," Lecture Notes in Computer Science (SPACE 2018), Vol. 11348, pp. 125-141, 2018.
7. Bernstein D. J., Birkner P., Joye M., Lange T., Peters Ch., "Twisted Edwards Curves," Progress in Cryptology - Africacrypt, LNCS 5023, pp. 389-405, 2008.
8. Bernstein D. J., Lange T., "Faster Addition and Doubling on Elliptic Curves," Progress in Cryptology - Africacrypt, LNCS 4833, pp. 29-50, 2007.
9. Bessalova A. V., Tsygankova O. V., "Number of Curves in the Generalized Edwards Form with Minimal Even Cofactor," Problems of Information Transmission, Vol. 53, Issue 1, pp. 92-101, 2017.
10. Bianco G., Gorla E., "Compression for Trace Zero Points on Twisted Edwards Curves," Journal of Mathematical Cryptology, Vol. 10, Issue 1, pp. 15-34, 2016.
11. Boneh, D., & Shoup, V. (2020). A Graduate Course in Applied Cryptography. Stanford University.
12. Buchmann, J. (2004). Introduction to Cryptography. Springer.
Childs, L. N. (2009). A Concrete Introduction to Higher Algebra. Springer.
13. Diffie, W., & Hellman, M. (1976). New Directions in Cryptography. IEEE Transactions on Information Theory, 22(6), 644-654.
14. Dugardin M., Guilley S., Moreau M., Najm Z., Rauzy P., "Using a Modular Extension to Protect Edwards Curves Against Fault Attacks," Journal of Cryptographic Engineering, Vol. 7, pp. 321-330, 2017.
15. Edwards H., "A Normal Form for Elliptic Curves," Bulletin of the American Mathematical Society, Vol. 44, Issue 3, pp. 393-422, 2007.
16. Fournaris A. P., Dimopoulos C., Moschos A., Koufopavlou O., "Design and Leakage Assessment of Side-Channel Resistant Binary Edwards ECDSA Architectures," Microprocessors and Microsystems, Vol. 64, pp. 73-87, 2019.
17. Hu Z., Gnatyuk S., Kovtun M., Seilova N., "Method of Searching Birationally Equivalent Edwards Curves over Binary Fields," Advances in Computer Science for Engineering and Education, pp. 309-319, 2019.
18. Kahn Academy. Cryptography and Number Theory. Educational resource materials.
19. Karthikeyan S., Jagadeeswari M., "Performance Improvement of ECC Using Low-Power High-Speed Vedic Multipliers," *Journal of Ambient Intelligence and Humanized Computing*, Vol. 12, Issue 3, pp. 4161-4170, 2020.
20. Katz, J., & Lindell, Y. (2015). Introduction to Modern Cryptography. Chapman and Hall/CRC.
21. Katz, J., & Lindell, Y. (2020). Introduction to Modern Cryptography (3rd ed.). CRC Press.
Koblitz, N. (1987). Elliptic Curve Cryptosystems. Mathematics of Computation, 48(177), 203-209.
Koblitz, N. (1994). A Course in Number Theory and Cryptography (2nd ed.). Springer-Verlag.
Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.
22. Kim S., Yoon K., Kwon J., Park Y. H., Hong S., "New Hybrid Method for Isogeny-Based Cryptosystems using Edwards Curves," Journal of LaTeX Class Files, Vol. 14, Issue 8, pp. 1-10, 2015.
23. Kim S., Yoon K., Park Y., Hong S., "Optimized Method for Computing Odd-Degree Isogenies on Edwards Curves," Advances in Cryptology - ASIACRYPT 2019, pp. 273-292, 2019.
24. Koblitz N., "Elliptic Curve Cryptosystems," Mathematics of Computation, Vol. 48, pp. 203-209, 1987.
25. Maharaja J. S. S. B. K. T., "Vedic Mathematics or Sixteen Simple

Paper received: 14.12.2025 Reviewed: 20.12.2025 Accepted: 28.12.2025 Published: 02.01.2026

Mathematical Formulae from Veda," Motilal Banarsidas, Varanasi, 1965.

26. Manoj Kumar, Ankur Kumar, "A Literature Survey on Vedic Mathematics Sutras for ECC," International Journal of Research in Electronics & Computer Engineering, Vol. 7, Issue 2, pp. 1635-1644, 2019.

27. Manoj Kumar, Ankur Kumar, "Algorithms of Projective Coordinate Systems for ECC Using Vedic Mathematics," International Journal of Scientific & Technology Research, Vol. 8, Issue 8, pp. 611-621, 2019.

28. Manoj Kumar, Ankur Kumar, "Efficient and Enhanced Techniques of Ancient Mathematics for ECC," International Journal of Information Technology & Electrical Engineering, Vol. 8, Issue 5, pp. 1-7, 2019.

29. Manoj Kumar, Ankur Kumar, "Improved Cryptographic Schemes Based on Hessian and Twisted Hessian Curves Using AIVM," International Journal of Advanced Science and Technology, Vol. 29, Issue 4, pp. 10190-10202, 2020.

30. Manoj Kumar, Ankur Kumar, "Improved Performance of Cryptosystem Based on Edwards and Twisted Edwards Curves using AIVM," Journal of Critical Reviews, Vol. 7, Issue 19, pp. 5787-5799, 2020.

31. Manoj Kumar, Ankur Kumar, "Performance Analysis of Huff and Twisted Huff Curves Using AIVM Techniques," Journal of Advances in Mathematics: Scientific Journal, Vol. 9, Issue 9, pp. 7191-7199, 2019.

32. Manoj Kumar, Ankur Kumar, "Sutras of Vedic Mathematics for ECC over Jacobian Coordinates," Journal of Analysis and Computation, Vol. 12, Issue 1, pp. 1-13, 2019.

33. Manoj Kumar, Ankur Kumar, "Techniques of Vedic Mathematics for ECC over the Ring A4," International Journal of Computer Sciences and Engineering, Vol. 7, Issue 5, pp. 1330-1337, 2019.

34. Manoj Kumar, Ankur Kumar, "The Tri-Linear Pairing Map Scheme for ECC Using Vedic Mathematics," International Journal of Information Technology & Electrical Engineering, Vol. 8, Issue 3, pp. 83-89, 2019.

35. Manoj Kumar, Sudhanshu Shekhar Dubey, Ankur Kumar, "Order of Convergence by Summation Integral Type Operators," International Journal of Computer & Mathematical Sciences, Vol. 7, Issue 1, pp. 66-79, 2018.

36. Manoj Kumar, Sudhanshu Shekhar Dubey, Ankur Kumar, "Simultaneous Approximation by Mixed Summation Integral Type Operators," International Journal of Innovations & Advancement in Computer Science, Vol. 7, Issue 3, pp. 71-79, 2018.

37. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.

38. Miller V. S., "Use of Elliptic Curves in Cryptography," Advances in Cryptology - CRYPT'85, LNCS 218, pp. 417-426, 1986.

39. Miller, V. S. (1985). Use of Elliptic Curves in Cryptography. Advances in Cryptology RYPTO '85 Proceedings. Springer.

40. Moody D., "Mean Value Formulas for Twisted Edwards Curves, Journal of Combinatorics and Number Theory, Vol. 3, Issue 2, pp. 1-11, 2010.

41. National Institute of Standards and Technology (NIST). (2015). Digital Signature Standard (DSS), FIPS PUB 186-4.

42. National Institute of Standards and Technology (NIST). (2023). Post-Quantum Cryptography Standardization Project.

43. Paar, C., & Pelzl, J. (2010). Understanding Cryptography: A Textbook for Students and Practitioners. Springer.

44. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2), 120-126.

45. Rosen, K. H. (2011). Elementary Number Theory and Its Applications. Pearson Education.

46. Schneier, B. (2015). Applied Cryptography. John Wiley & Sons.

47. Shirase M., "Coordinate System for Elliptic Curve Cryptosystem on Twisted Edwards Curve," International Conference on Consumer Electronics-Taiwan, pp. 1-6, 2016.

48. Shor, P. W. (1994). Algorithms for Quantum Computation: Discrete Logarithms and Factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS), 124-134.

Paper received: 14.12.2025 **Reviewed: 20.12.2025** **Accepted: 28.12.2025** **Published: 02.01.2026**

49. Singh, S. (1999). The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Anchor Books.
50. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson Education.
51. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.).
52. Trappe, W., & Washington, L. C. (2006). Introduction to Cryptography with Coding Theory. Pearson.
53. Yu W., Wang K., Li B., He X., Tian S., "Deterministic Encoding into Twisted Edwards Curves," ACISP 2016, LNCS 9723, pp. 285-297, 2016.

Paper received: 14.12.2025 Reviewed: 20.12.2025 Accepted: 28.12.2025 Published: 02.01.2026