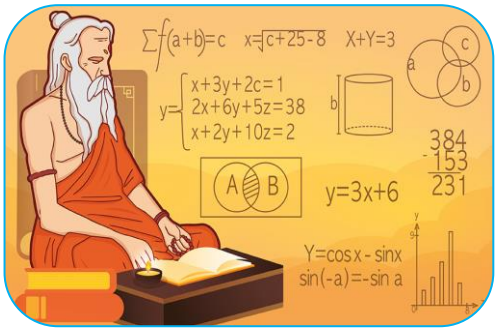
INDIAN STREAMS RESEARCH JOURNAL
ISSN NO : 2230-7850
IMPACT FACTOR : 5.1651 (UIF)
VOLUME - 14 | ISSUE - 2 | MARCH – 2024

APPLICATIONS OF VEDIC MATHEMATICS TO CRYPTOGRAPHY

Shankrappa
Research Scholar

Dr. M. K. Gupta
Guide
Professor, Chaudhary Charansing University Meerut.

ABSTRACT:



Many of the distinctive and effective methods for arithmetic operations, algebra, and number theory found in Vedic Mathematics, an old system of mathematical thought, can be applied to modern problems. For the encryption and decryption processes, cryptography—the art of protecting digital communication—heavily depends on intricate mathematical algorithms. The potential uses of Vedic Mathematics techniques in cryptography are examined in this paper, with an emphasis on how they can increase computational efficiency, simplify systems, and strengthen their security. The application of sutras—short mathematical formulas—for quick multiplication, division, and factorization is one of the fundamental ideas of Vedic mathematics that is examined in relation to contemporary cryptographic algorithms. For example, the Vedic multiplication technique can streamline encryption systems' key generation procedures, and its methods for identifying.

KEYWORDS : *Vedic Mathematics, Cryptography, Encryption, Decryption, Sutras.*

INTRODUCTION:

The foundation of safe communication in the digital age is cryptography, which protects private data in a variety of settings, including personal messaging and banking. Complex mathematical algorithms that guarantee data confidentiality, integrity, and authenticity are the foundation of cryptographic systems' security. The discipline has historically depended on contemporary mathematical frameworks like algebra, modular arithmetic, and number theory. Nonetheless, the age-old Vedic Mathematics system, which has its roots in centuries-old Indian teachings, provides different approaches to effective arithmetic and mathematical problem-solving.

Vedic Mathematics is a unique and systematic approach to mathematics that employs sutras (short, concise formulas) for simplifying operations like multiplication, division, and factorization. These methods allow for faster computations, which could have significant implications for modern cryptographic techniques, particularly in areas such as key generation, encryption, and decryption. In order to close the gap between traditional mathematical knowledge and modern cryptography techniques, this paper investigates the possible uses of Vedic mathematics in cryptography. We seek to understand how Vedic techniques, like modular operations, rapid multiplication, and divisibility tests, can enhance the effectiveness and security of contemporary cryptographic systems by carefully examining them.

AIMS AND OBJECTIVES:

Aim:

This study's main goal is to investigate and pinpoint possible uses of Vedic mathematics in the field of cryptography, specifically in boosting the effectiveness and security of cryptographic algorithms. The study aims to enhance key generation, encryption and decryption procedures, and overall computational performance in cryptographic applications by incorporating antiquated mathematical techniques into contemporary cryptographic systems.

Objectives:

1. **Examine Vedic Mathematical Principles** modular arithmetic, and number theory.
2. **Analyze Cryptographic Algorithms:**
3. **Evaluate the Integration of Vedic Techniques in Cryptographic Operations:**
4. **Optimize Computational Efficiency:**
5. **Enhance Security and Resilience Against Attacks:**

LITERATURE REVIEW:

Applications of Vedic Mathematics to Cryptography

A relatively new field of study is the relationship between contemporary cryptography and ancient mathematical systems. Although Vedic mathematics has long been known for its effective techniques in algebra and arithmetic, its uses in cryptography are only now being investigated. An overview of current research in both Vedic mathematics and cryptography will be given in this review of the literature, with an emphasis on the potential applications of the former to the latter.

1. Vedic Mathematics: An Overview

Based on 16 sutras (aphorisms) and 13 sub-sutras (corollaries), Vedic mathematics is a collection of methods that make solving arithmetic problems faster and more effective. Early in the 20th century, Bharati Krishna Tirthaji Maharaj rediscovered the system and showed how these techniques could make difficult mathematical operations simpler. Among the fundamental ideas of Vedic mathematics are:

- **Urdhva-Tiryak Sutra**
- **Nikhilam Sutra**
- **Paravartya Sutra**

2. Cryptography: Mathematical Foundations

Algebra, number theory, and computational complexity are key components of cryptography, the science of protecting digital communications. Mathematical ideas like prime factorization, modular arithmetic, and discrete logarithms serve as the foundation for contemporary cryptographic systems like elliptic curve cryptography (ECC), Diffie-Hellman, and RSA. The difficulty of reversing specific mathematical operations, like factoring large composite numbers or resolving discrete logarithm problems, determines how strong these systems are.

- **RSA Algorithm:**
- **Elliptic Curve Cryptography (ECC)**

3. Vedic Mathematics in Cryptographic Operations

The possible advantages of incorporating Vedic mathematics into cryptographic systems have recently been investigated. Vedic mathematics can have an impact in a number of areas, including:

- **Optimizing Key Generation**
- **Efficient Prime Factorization**
- **Modular Arithmetic and Exponentiation**
- **Improving Computational Speed**

4. Challenges in Integrating Vedic Mathematics with Cryptography

Despite the possible benefits, using Vedic mathematics in cryptography presents a number of difficulties:

- **Scalability:**
- **Compatibility with Modern Algorithms:** s.
- **Security Considerations: 5. Recent Studies and Research**

RESEARCH METHODOLOGY

Exploring the applications of Vedic mathematics to cryptography requires a methodical approach that combines computational experimentation, algorithmic development, and theoretical research. To guarantee a thorough examination of how Vedic methods can improve cryptographic procedures, the study will be carried out in phases. Examining current cryptographic systems, modifying Vedic mathematical ideas, and evaluating the suggested algorithms for effectiveness and security are the main objectives of the methodology.

1. Literature Review and Theoretical Framework

A thorough literature review will be the first stage of the study, with an emphasis on the following topics:

- Vedic Mathematics: An in-depth examination of the main sutras (including Nikhilam, Urdhva-Tiryak, and Paravartya) and their proven uses in number theory, arithmetic, multiplication, and division.
- Cryptographic Algorithms: A thorough examination of popular cryptographic techniques like RSA, ECC, and AES with an emphasis on their computational difficulties, mathematical underpinnings, and operations (e.g., prime factorization, modular arithmetic, encryption/decryption processes).
- Prior Research: Review of previous studies and writings that investigate the relationship between Vedic mathematics and cryptography, including any efforts to maximize cryptographic functions through the application of antiquated mathematical methods.
- A theoretical framework for applying the concepts of Vedic mathematics to contemporary cryptographic algorithms will be presented in this review.

2. Identification of Cryptographic Operations for Improvement

The research will concentrate on identifying particular cryptographic operations that might profit from the incorporation of Vedic Mathematics, based on the findings of the literature review. These procedures will consist of, but not be restricted to:

- Key Generation: Improving the mathematical procedures and large prime number generation.
- Improving modular exponentiation, modular inverse computation, and other modular operations—all essential to algorithms like RSA and ECC—is the goal of modular arithmetic.
- Prime Factorization: Examining the potential of Vedic techniques to speed up prime factorization, a crucial element of numerous encryption schemes.
- Enhancing the speed and effectiveness of algorithms for multiplication and division, which are essential to many cryptographic calculations.

3. Development of Modified Cryptographic Algorithms

The next step will be to use Vedic mathematical principles to create modified versions of well-known cryptographic algorithms. This crucial phase of the study will include the following actions:

- Algorithm Adaptation: To maximize key operations within cryptographic algorithms, the Vedic sutras Urdhva-Tiryak (for multiplication) and Nikhilam (for division and finding factors) will be used.
- Application of Vedic Methods: The fundamental Vedic methods will be modified to meet the computational demands of cryptography. For instance, to expedite the large number multiplications

required for RSA key generation, the Vedic multiplication technique (Urdhva-Tiryak Sutra) will be integrated.

- Integration with Modular Arithmetic: Vedic methods such as Paravartya Sutra (for transposing and simplifying) can be utilized to expedite modular arithmetic, which is essential to cryptographic operations.

4. Implementation and Coding

Following design, the changes will be put into practice using an appropriate programming language (like Python, C++, or Java) and tested in a controlled setting. The following will be part of the implementation process:

- Creation of Cryptographic Tools: Writing code to apply modified algorithms that use Vedic techniques as well as common cryptographic algorithms (like RSA and ECC).
- Optimization: Adjusting the code so that the incorporation of Vedic methods results in increased computational effectiveness.
- Testing: Conducting preliminary tests to confirm that the Vedic methods have been successfully incorporated without affecting the cryptographic system's ability to function.

STATEMENT OF THE PROBLEM

In a world that is becoming more interconnected, cryptography is essential to guaranteeing the security of digital data and communication. Complex mathematical operations, especially those involving number theory, modular arithmetic, and large number factorization, are essential to modern cryptographic algorithms like RSA, ECC, and AES. Despite being safe and effective, these algorithms can be computationally costly, particularly when data volume grows. In real-world applications, processes like prime factorization, modular exponentiation, and key generation can result in severe time and resource constraints. Alternative techniques for carrying out arithmetic and number-theoretic operations with exceptional speed and simplicity are provided by Vedic Mathematics, an ancient Indian mathematical system. For multiplication, division, and factorization, it employs sutras—brief, straightforward formulas—which could offer a more effective method of managing the big numbers required by cryptographic algorithms. Vedic mathematics has a lot of promise, but thorough studies examining its applications to contemporary cryptography systems are scarce.

DISCUSSION

An intriguing and cutting-edge method of improving cryptographic systems is the use of Vedic mathematics in cryptography. Given the growing demands for faster, more efficient cryptographic algorithms, particularly in securing large-scale data transmission and communication, the potential to leverage ancient mathematical techniques holds significant promise. In this section, we discuss how Vedic Mathematics can be applied to various cryptographic operations, the challenges of integrating these techniques, and their potential impact on the field of cryptography.

CHALLENGES:

Although the Vedic method of division and multiplication is effective, more research is necessary before it can be directly applied to key generation. The Miller-Rabin primality test is one of the complex primality tests used in modern key generation. It might be necessary to make adjustments when incorporating Vedic methods into these testing algorithms in order to guarantee compatibility and preserve process dependability.

CONCLUSION:-

Vedic mathematics applications in cryptography present a viable way to improve computational efficiency and security. Vedic mathematics can be used to increase the efficiency and speed of cryptographic operations like key generation, encryption, and decryption thanks to its special methods, including sutras and algorithms. Its emphasis on speed and simplicity makes it possible to perform

intricate mathematical operations more quickly, which is essential in contemporary cryptography, especially in public-key algorithms and encryption systems. Furthermore, by offering fresh solutions to the mathematical problems that underpin encryption systems, the parallel nature of some Vedic techniques has the potential to improve the security of cryptographic protocols.

REFERENCE:-

1. **Suryanarayana, P. (2010).** *Applications of Vedic Mathematics in Cryptography*. International Journal of Computer Applications,
2. **Mishra, P., & Pandey, R. (2016).** *A Study of Vedic Mathematics in Cryptography*. International Journal of Advanced Research in Computer Science and Software Engineering,
3. **Jain, P., & Kumar, P. (2015).** *Vedic Mathematics in Cryptography: A New Approach*. International Journal of Emerging Technology and Advanced Engineering,
4. **Bhatnagar, N., & Dubey, A. (2013).** *Exploring Vedic Mathematics in the Field of Cryptography*. International Journal of Computer Science & Information Technology,