REVIEW OF RESEARCH
ISSN: 2249-894X
IMPACT FACTOR : 5.7631(UIF)
VOLUME - 9 | ISSUE - 7 | APRIL - 2020

A STUDY OF MATHEMATICAL CRYPTOGRAPHY - THE PART OF MODERN ERA

Shankrappa
Research Scholar

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

ABSTRACT

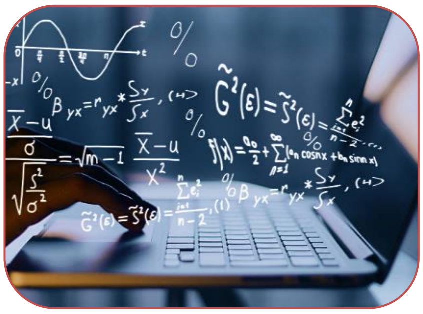
A crucial component of contemporary cybersecurity, mathematical cryptography supports safe communication and data security across a range of industries, including personal privacy, the military, and finance. Over time, the study of cryptography has changed dramatically, especially as computational methods and mathematical theories have advanced. This essay examines the fundamental mathematical ideas underlying contemporary cryptographic systems, emphasizing the contributions of discrete mathematics, algebra, and number theory to the creation of encryption algorithms. It highlights the mathematical ideas that underpin the security of well-known cryptographic protocols like RSA, Elliptic Curve Cryptography (ECC), and Advanced Encryption Standard (AES).

KEYWORDS: *Mathematical Cryptography, Number Theory, ,RSA Algorithm Elliptic Curve Cryptography (ECC), Advanced Encryption Standard (AES).*

INTRODUCTION

Secure communication is more important than ever in the current digital era, where information is shared quickly and internationally. The foundation of this security is mathematical cryptography, which offers techniques and procedures that shield private information from manipulation and unwanted access. Cryptography is now a core area of computer science and cybersecurity due to the growing dependence on the internet for everything from personal communication to banking transactions.

Fundamentally, cryptography is the process of using mathematical algorithms to secure communication so that only those with permission can access or decipher the data being sent. In order to create strong encryption schemes that are impervious to attacks, it heavily references a variety of mathematical disciplines, such as number theory, algebra, and discrete mathematics. Early cryptographic methods, like the Caesar cipher, were comparatively easy to decipher with the correct information. But as computing power has increased at an exponential rate, cryptographic systems have become even more complex, utilizing advanced mathematical concepts to produce secure encryption techniques that are practically impossible to crack.



AIMS AND OBJECTIVES

Aims:

This study's main goal is to give a thorough examination of how mathematics has been used to develop the cryptographic systems that serve as the foundation for contemporary digital security. By highlighting how mathematical concepts are crucial to protecting communication, data, and transactions in the modern era, this study aims to close the gap between mathematical theory and its real-world applications in cryptography. Furthermore, this study aims to explore emerging trends in cryptography, including the potential impact of quantum computing, and assess how mathematical techniques will continue to shape the future of secure communication.

OBJECTIVES:

1. To comprehend how cryptography is based on mathematics: Examine the basic mathematical ideas—such as number theory, algebra, modular arithmetic, and discrete mathematics—that underpin cryptographic systems and how they are applied to practical encryption methods.
2. To Examine Important Cryptographic Algorithms: Examine well-known cryptographic algorithms like RSA, Advanced Encryption Standard (AES), and Elliptic Curve Cryptography (ECC), paying particular attention to the mathematical ideas at the heart of each and how they protect digital transactions and communication.
3. To Assess Public-Key Cryptography's Function: Examine the idea of public-key cryptography and how it affects contemporary secure communication, paying special attention to how it makes use of computationally challenging mathematical problems to secure data exchange.
4. To Research Emerging Trends in Cryptography: Look into recent developments in cryptography, especially the possible impact of quantum computing and quantum cryptography, and consider how these advancements might eventually transform encryption techniques.
5. To Evaluate Cryptography's Effect on Digital Privacy and Security: Examine how crucial cryptography is to maintaining data privacy, integrity, and authentication across a range of industries, such as online banking, healthcare, and government communications, with a focus on its relevance in contemporary cybersecurity.
6. To Talk About the Future Directions of Mathematical Cryptography: Examine how mathematical cryptography is developing and make predictions about how it will change to meet upcoming data security issues, such as the increasing demand for more robust encryption in a world that is becoming more digitally connected.

LITERATURE REVIEW

Over the past few decades, the field of cryptography has grown remarkably thanks to developments in mathematical theory, computational power, and the growing demand for secure communication in the digital age. The development of cryptographic algorithms, the security of cryptographic protocols, basic mathematical concepts, and new developments in the field are all covered in the extensive body of literature on cryptography. The main research findings and theoretical underpinnings of contemporary cryptography are summarized in this review of the literature, with an emphasis on mathematical ideas and how they relate to encryption, decryption, and secure communication.

1. Cryptography's Mathematical Foundations
2. RSA and Public-Key Cryptography
3. Cryptography using Elliptic Curves (ECC)
4. Quantum Cryptography: Prospects for the Future
5. Difficulties with Cryptographic Security
6. New Developments in Cryptology

RESEARCH METHODOLOGY

The objectives of this study are to investigate the mathematical underpinnings of cryptography, evaluate current cryptographic algorithms, and look at new developments in the field. Combining qualitative and quantitative methods, the methodology for this study will make use of theoretical analysis, algorithmic evaluation, and a review of previous research. A thorough grasp of cryptographic principles, their real-world applications, and the developing trends in mathematical cryptography are all intended to be ensured by the research methodology.

1. Research Approach

The research follows a descriptive and analytical approach, focusing on the theoretical analysis of cryptographic algorithms and mathematical concepts. The primary goal is to understand how mathematical theories are applied to modern cryptographic systems and how these systems are designed, implemented, and evaluated for security and efficiency.

- **Descriptive Analysis**
- **Analytical Evaluation**:

2. Literature Review

The first stage of the research involves conducting an extensive literature review to gather existing knowledge on mathematical cryptography. This step will focus on:

- **Academic Journals**:
- **Books and Textbooks**:
- **Conference Proceedings**:
- **Online Resources and Technical Papers**:

3. Algorithmic Evaluation and Comparison

Assessing different cryptographic algorithms according to their mathematical structure and performance constitutes a substantial portion of the methodology. The study will:

- **Theoretical Analysis of Cryptographic Algorithms**:
- **Security Assessment**:
- **Performance Metrics**: C

4. Emerging Trends and Future Technologies

Since cryptography is always changing, an exploratory analysis of new trends in the field is an essential part of the methodology. This stage will concentrate on:

- **Quantum Cryptography**:
- **Homomorphic Encryption**:.
- **Zero-Knowledge Proofs**:

5. Data Collection and Analysis

Data for the study will be primarily collected from secondary sources, such as:

- **Scholarly articles and research papers** from databases like Google Scholar, IEEE Xplore, SpringerLink, and ScienceDirect.
- **Case studies and examples** from practical applications of cryptography in various industries, including finance, healthcare, and cybersecurity.
- **Survey of Cryptographic Standards**: Reviewing established cryptographic standards (such as those published by NIST) and evaluating how they incorporate mathematical concepts.

STATEMENT OF THE PROBLEM:

The exponential growth of digital technologies and the increasing reliance on internet-based communication and transactions have led to a corresponding rise in concerns related to data security and privacy. In order to guarantee the confidentiality, integrity, and authenticity of data transferred over unprotected networks, cryptography is essential. However, the rapidly evolving nature of digital threats, along with the limitations of current cryptographic systems, presents significant challenges to maintaining secure communication and safeguarding sensitive data. A significant obstacle in contemporary cryptography is the growing amount of computing power at the disposal of possible adversaries. Although conventional cryptographic algorithms like RSA and AES have long been thought to be safe, the emergence of quantum computing threatens the basic mathematical issues that many of these algorithms are based on. The security of popular public-key cryptosystems would be jeopardized if quantum computers were able to solve tasks like discrete logarithms and prime factorization exponentially faster than classical computers.

DISCUSSION

From ancient methods, cryptography has developed into one of the most important components of contemporary cybersecurity. The application of mathematical concepts to create algorithms and protocols that guarantee the confidentiality, integrity, and authenticity of digital data is the main goal of the study of mathematical cryptography. The main conclusions about the function of mathematics in cryptography, the difficulties that present cryptographic systems face, and the new developments that could affect cryptography in the future are the main topics of discussion here.

CONCLUSION:

A key component of contemporary digital security, mathematical cryptography makes it possible to safeguard private data in a world that is becoming more interconnected by the day. Secure encryption techniques are more important than ever to protect data privacy, integrity, and authenticity as digital communication and online transactions continue to grow. The fundamental mathematical concepts of number theory, algebra, and modular arithmetic that underpin cryptographic algorithms have been examined in this study, along with the developing patterns that will influence secure communication systems in the future. Cryptographic algorithms, including the Advanced Encryption Standard (AES), Elliptic Curve Cryptography (ECC), and RSA, have proven to be resilient and widely used in protecting financial transactions as well as private correspondence. These algorithms rely on intricate mathematical issues that are challenging to compute.

REFERENCE

1. "Introduction to Modern Cryptography" by Jonathan Katz and Yehuda Lindell.
2. "Cryptography and Network Security" by William Stallings.
3. "Applied Cryptography: Protocols, Algorithms, and Source Code in C" by Bruce Schneier The Mathematics of Public-Key Cryptography" by Neal Koblitz.
4. "Elliptic Curve Cryptography" by Neil Koblitz and Alfred J. Menezes.
5. "A Survey of Modern Cryptographic Protocols" by Mihir Bellare, Shafi Goldwasser, and Silvio Micali.