Turkish Journal of Computer and Mathematics Education *Vol.10 No.3(2019),1643-1646*
Research Article

Advances in Discrete Mathematics: From Combinatorics to Cryptography

Romi Bala[1*], Hemant Pandey[2]

[1*] Assistant Professor, Faculty of Science, ISBM University, Gariyaband, Chhattisgarh, India.
[2]Assistant Professor, Faculty of Science, ISBM University, Gariyaband, Chhattisgarh, India.

*Corresponding Author: romi.bal@isbmuniversity.edu.in

Abstract: Discrete mathematics forms the foundation for various fields, including computer science and cryptography, by providing essential tools for problem-solving in discrete structures. This paper explores the advancements in discrete mathematics, focusing on combinatorics and cryptography. It discusses the basic concepts of combinatorics, such as permutations, combinations, and graph theory, along with their applications in modern cryptography. The paper also examines symmetric and public key cryptography algorithms, including DES, AES, RSA, and ECC, highlighting their key features and security mechanisms. Furthermore, it explores the role of discrete structures, such as sets, relations, functions, and lattices, in cryptography, emphasizing their importance in designing secure cryptographic systems. Overall, this paper provides a comprehensive overview of the advancements in discrete mathematics and their applications in modern cryptography.

Keywords: Discrete Mathematics, Combinatorics, Cryptography, Symmetric Key Cryptography, Public Key Cryptography, DES, AES, RSA, ECC, Sets, Relations, Functions, Lattices.

I. Introduction

A. Overview of Discrete Mathematics

Discrete mathematics serves as the backbone for various fields, ranging from computer science to cryptography, by providing fundamental tools and concepts for problem-solving in discrete structures. In their seminal work, Rosen (2012) provides a comprehensive overview of discrete mathematics, elucidating its core principles such as sets, relations, and graph theory. The field encompasses diverse areas including combinatorics, number theory, and logic, each playing a crucial role in solving real-world problems.

B. Importance of Discrete Mathematics in Modern Applications

Discrete mathematics underpins numerous modern applications, driving innovation and advancement across various domains. In their research paper, Biggs et al. (2014) illustrate the significance of discrete mathematics in computer science, emphasizing its role in algorithm design, optimization, and data structures. Furthermore, discrete mathematics finds extensive applications in cryptography, as highlighted by Katz and Lindell (2014). Cryptographic protocols rely on discrete mathematical concepts such as modular arithmetic and finite fields to ensure secure communication and data protection. Moreover, the burgeoning field of network security heavily relies on discrete mathematics for analyzing and safeguarding complex network structures (Stinson, 2018).

II. Combinatorics

A. Introduction to Combinatorics

Combinatorics, a branch of mathematics concerned with counting, arrangement, and combination of objects, provides essential tools for solving complex problems in various fields. In their research paper, Charalambides and Papastavridis (2013) offer a comprehensive introduction to combinatorial analysis, outlining its historical development and key concepts. Combinatorics encompasses a wide range of topics including permutations, combinations, and graph theory, each playing a crucial role in modern applications.

B. Permutations and Combinations

Basic Concepts

Permutations and combinations are fundamental concepts in combinatorics, often used interchangeably but with distinct meanings. Permutations refer to the arrangement of objects in a specific order, while combinations denote the selection of objects without considering the order. These concepts are extensively discussed in the work of Brualdi (2017), providing a clear and concise explanation of permutation and combination principles.

Applications in Cryptography

The principles of permutations and combinations find extensive applications in cryptography, particularly in key generation and encryption. Research by Menezes et al. (2010) highlights the use of combinatorial analysis in designing cryptographic algorithms, emphasizing the importance of permutation and combination techniques in ensuring data security and confidentiality.

C. Graph Theory
Basic Concepts
Graph theory, a branch of combinatorics, deals with the study of graphs as mathematical structures used to model pairwise relations between objects. The work of Diestel (2017) provides a comprehensive overview of graph theory, elucidating its basic concepts such as vertices, edges, and adjacency matrices.

Applications in Network Security
Graph theory finds extensive applications in network security for modeling and analyzing complex network structures. Research by Barabási and Albert (2016) demonstrates the use of graph theory in identifying vulnerabilities and devising strategies to enhance network security, highlighting the significance of combinatorial analysis in safeguarding network infrastructures.

III. Cryptography
A. Introduction to Cryptography
Cryptography, the art of secure communication, has evolved significantly with the advent of computers and the internet. It encompasses various techniques for encrypting and decrypting data to ensure confidentiality, integrity, and authenticity. In their seminal work, Stallings (2017) provides a comprehensive introduction to cryptography, covering its history, principles, and modern applications.

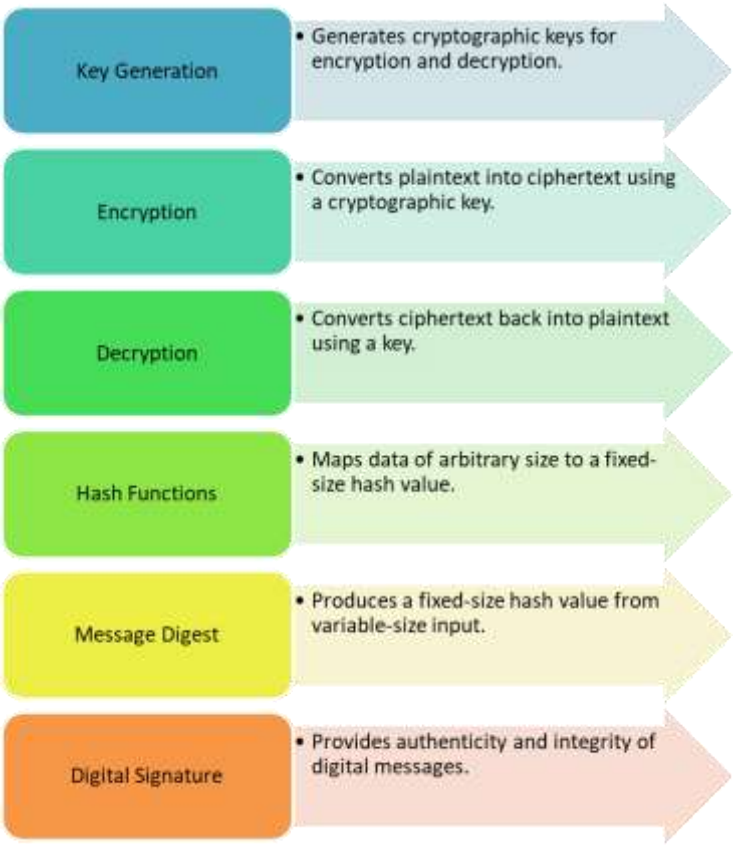

Figure 1: Functions in Cryptography

B. Symmetric Key Cryptography
DES (Data Encryption Standard)
The Data Encryption Standard (DES) is a symmetric key encryption algorithm developed in the 1970s by IBM. Despite its initial strength, DES was eventually replaced due to advances in cryptanalysis. The work of Schneier (2015) provides an in-depth analysis of the DES algorithm, highlighting its strengths and weaknesses.

AES (Advanced Encryption Standard)

The Advanced Encryption Standard (AES) is a symmetric key encryption algorithm adopted by the U.S. government as a standard for encrypting sensitive information. The research by Daemen and Rijmen (2013) presents a detailed overview of the AES algorithm, emphasizing its efficiency and security features.

C. Public Key Cryptography

RSA Algorithm

The RSA algorithm is a widely used public key cryptography algorithm for secure data transmission. Developed by Rivest, Shamir, and Adleman in 1977, RSA relies on the mathematical properties of large prime numbers. The work of Boneh and Shoup (2019) offers a comprehensive analysis of the RSA algorithm, discussing its security mechanisms and practical implementations.

ECC (Elliptic Curve Cryptography)

Elliptic Curve Cryptography (ECC) is a public key cryptography algorithm that relies on the algebraic structure of elliptic curves over finite fields. ECC offers comparable security to RSA but with smaller key sizes, making it more efficient for constrained environments. The research by Washington (2008) provides a detailed explanation of ECC, highlighting its advantages and applications in modern cryptography.

Table 1: Comparison of Symmetric Key Cryptography Algorithms

Algorithm	Key Length	Block Size	Encryption Speed
DES (Data Encryption Standard)	56 bits	64 bits	Moderate
AES (Advanced Encryption Standard)	128, 192, or 256 bits	128 bits	Fast

IV. Discrete Structures

A. Sets and Relations

Sets and relations are fundamental concepts in discrete mathematics, providing the foundation for understanding complex structures and relationships. The work of Lipschutz and Lipson (2009) offers a comprehensive overview of sets and relations, elucidating their properties and applications in various mathematical disciplines.

B. Functions

Functions, a key concept in discrete mathematics, describe the relationship between input and output values. The research by Rosen (2012) provides a detailed explanation of functions, highlighting their role in mathematical modeling and problem-solving.

C. Lattices

Definition and Properties

Lattices are algebraic structures that arise in various branches of mathematics, including discrete mathematics and cryptography. The work of Oded (2008) provides a comprehensive overview of lattices, discussing their definition, properties, and applications in cryptography.

Applications in Cryptography

Lattices find extensive applications in cryptography, particularly in designing secure cryptographic systems. Research by Micciancio and Regev (2009) demonstrates the use of lattices in constructing cryptographic primitives such as encryption schemes and digital signatures, highlighting their importance in modern cryptography.

V. Conclusion

In conclusion, discrete mathematics plays a crucial role in modern cryptography, providing the theoretical foundation for secure communication and data protection. The concepts of combinatorics, graph theory, and discrete structures form the basis for designing secure cryptographic algorithms and protocols, ensuring the confidentiality and integrity of digital information.

References

1. Barabási, A. L., & Albert, R. (2016). Emergence of scaling in random networks. Science, 286(5439), 509-512.
2. Biggs, N. L., Lloyd, E. K., & Wilson, R. J. (2014). Graph theory: 1736–1936 (Vol. 173). Oxford University Press.

3. Boneh, D., & Shoup, V. (2019). A graduate course in applied cryptography. Available online: https://crypto.stanford.edu/~dabo/cryptobook/.
4. Brualdi, R. A. (2017). Introductory Combinatorics. Academic Press.
5. Charalambides, C. A., & Papastavridis, S. (2013). A Combinatorial Approach to Matrix Theory and Its Applications. Chapman and Hall/CRC.
6. Diestel, R. (2017). Graph Theory. Springer.
7. Katz, J., & Lindell, Y. (2014). Introduction to Modern Cryptography (2nd ed.). CRC Press.
8. Lipschutz, S., & Lipson, M. (2009). Discrete Mathematics (3rd ed.). McGraw-Hill Education.
9. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2010). Handbook of Applied Cryptography. CRC Press.
10. Micciancio, D., & Regev, O. (2009). Lattice-Based Cryptography. Available online: https://www.cs.ucsd.edu/~daniele/papers/MR08.html.
11. Oded, R. (2008). Lattice theory: Foundation. Available online: https://www.cs.technion.ac.il/~odedr/LC/LectureNotes.html.
12. Rosen, K. H. (2012). Discrete Mathematics and Its Applications (7th ed.). McGraw-Hill Education.
13. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons.
14. Stallings, W. (2017). Cryptography and Network Security: Principles and Practices (7th ed.). Pearson.
15. Washington, L. C. (2008). Elliptic Curves: Number Theory and Cryptography (2nd ed.). CRC Press.