Abstract No: 188 ***ICT, Mathematics, and Statistics***

AN APPLICATION OF GRAPH THEORY IN ASYMMETRIC KEY CRYPTOGRAPHY

K.K.N.Fernando* and G.S.Wijesiri

Department of Mathematics, Faculty of Science, University of Kelaniya, Kelaniya, Sri Lanka.
**kaveefdo97@gmail.com*

The development of digital communication in many facets of our everyday lives significantly impacts the evolving world we live in today. The rapid growth and evolution of digital communication have become the backbone of how we interact with other people. Therefore, it is imperative to protect information and data from unauthorised activities, such as accessing, using, exposing, damaging, modifying, copying, or deleting them. Safeguarding data from these invalid operations is crucial to ensure its integrity, confidentiality, and availability. Cryptography plays a pivotal role in ensuring the security and privacy of information in various contexts, such as online banking, e-commerce transactions, and communication between governments, military organisations, and businesses. Various types of mathematical techniques are available for application in modern cryptology. The application of graph theory is widely utilised in the field of cryptography due to its straightforward representation in computers as a matrix. In this study, we propose a novel asymmetric key cryptography scheme for secure message transmission using graph theory and matrices. The proposed scheme consists of four algorithms. The key generation algorithm on the receiver side is based on the properties of matrices, which enables us to establish the relationship between private key and public key through matrix operations. On the sender-side graph generation algorithm, a graph theory approach is applied to encrypt the original message, and the message is converted into a splitting graph and its minimum spanning tree. Then, the sender-side encryption algorithm is used to generate a complex final ciphertext using the receiver's public key. The decryption algorithm follows the same process in reverse order, employing the receiver's private key. This system will provide better security while storing data in the financial retail industry and sharing passwords in transactions.

Keywords: Asymmetric Cryptography, Cipher text, Cryptography, Decryption, Encryption