Abstract No. 64 ***Mathematics***

A NOVEL CRYPTOGRAPHIC SCHEME BASED ON RADIO MEAN LABELLING

G.H.S.N. Weerasinghe[1]* and A.A.I. Perera[2]

[1]Department of Physical Science, Faculty of Applied Sciences, Rajarata University of Sri Lanka, Mihintale, Sri Lanka
[2]Department of Mathematics, Faculty of Science, University of Peradeniya, Peradeniya, Sri Lanka
**nethmini1026@gmail.com*

Graph theory and cryptography have long been intertwined, offering powerful techniques for securing information across disciplines such as computer science, engineering, and biology. This study introduces a novel encryption and decryption algorithm that integrates Radio mean labelling of cycle graphs with a polyalphabetic cypher, aiming to bolster cryptographic security. Graph labelling assigns labels to graph elements, facilitating efficient data representation and manipulation. A radio labelling f of graph G assigns positive integers to the vertices of G such that $|f(u) - f(v)| \geq \text{diam}(G) + 1 - d(u, v)$, where $u, v \in V(G)$, $\text{diam}(G)$ represents the diameter of the graph, and $d(u, v)$ denotes the distance between vertices u and v. This definition is modified as $\lceil (f(u) + f(v)) / 2 \rceil \geq \text{diam}(G) + 1 - d(u, v)$, which is called the Radio Mean Labelling (RML) of G. The Radio Mean number of f, $\text{rmn}(f)$, is the maximum number assigned to any vertex of G. The Radio Mean number of G, $\text{rmn}(G)$, is the minimum value of $\text{rmn}(f)$ taken over all RMLs of G. In this approach, the plaintext is transformed into cyphertext using an alternative RML method applied to odd cycle graphs, specifically C_{2n+1}, combined with a polyalphabetic structure. The method assigns labels sequentially to odd cycles with odd or even diameters, selecting vertices from zero at maximum distance. Each label satisfies the Radio Mean condition relative to all previous labels, shaping the cypher. Decryption is achieved by utilizing two keys: the odd cycle graph and a keyword, enabling the accurate restoration of the original message. The polyalphabetic table is constructed using a shifting value, k, derived from the Radio mean number of the cycle graph and the length of the keyword. This method effectively enhances data security by integrating graph-based transformations with traditional encryption techniques. Future research will focus on extending this approach by incorporating different cycle graph structures and alternative graph labelling techniques to further improve encryption strength.

Keywords: Cryptography, Decryption, Encryption, Radio Mean Labelling