

AS/OP/03

A Cycle-Based Symmetric Encryption using Radio Arithmetic Mean Labeling and Extended Hill Cipher

Weerasinghe GHSN¹, Perera AAI²

¹*Department of Physical Sciences, Faculty of Applied Sciences, Rajarata University of Sri Lanka, Mihintale*

²*Department of Mathematics, Faculty of Science, University of Peradeniya, Peradeniya*

Graph labeling encodes numerical relationships within network structures. Applying distance constraints to these labelings offers a clear and organized way to create secure cryptographic algorithms. This study presents a symmetric encryption technique combining Radio Arithmetic Mean Labeling (RAML) on even cycle graphs with a structurally adaptive Hill cipher. RAML ensures that vertex labels satisfy the arithmetic mean condition; $\lceil (f(u) + f(v))/2 \rceil \geq \text{diam}(G) + 1 - d(u, v)$ where f is the labeling, u and v are vertices of the graph G , $d(u, v)$ denotes the distance between u and v , and $\text{diam}(G)$ represents the diameter of G . The highest value given during this process is called the Radio Mean Number (RMN). The encryption key is constructed from the labeling sequence of a chosen cycle graph, and the key matrix dimension is derived from the order and symmetry of the graph structure. The system incorporates an extended 36-symbol alphanumeric space, comprising uppercase English letters and digits, enabling broader data representation beyond conventional ciphers. Repeated characters in the plaintext are replaced by a substitution marker to avoid confusion during encryption. Message blocks are padded with placeholder values to match the required matrix dimensions. Numeric equivalents of these characters are arranged in blocks and processed using modular matrix multiplication. To enhance security, a RMN determined from the labeling process is optionally added to the transformed data to introduce a dynamic offset that is graph-dependent and resistant to simple cryptanalysis. Compared to classical methods such as the standard Hill cipher, this approach is more effective because RAML-guided labeling enables structured key generation, reducing key management complexity while maintaining strong encryption. Decryption is performed by reversing the process using the same RAML-based matrix and modular arithmetic. Future work includes expanding the method to handle irregular graphs and looking into multi-layered cryptographic applications, like secure communication and dynamic key management.

Keywords: Cryptography, Hill Cipher, Radio Arithmetic Mean Labeling