Abstract No: PO-36

Symmetric key encryption and decryption using graph theory

K. K. N. Fernando[1*], G. S. Wijesiri[1]

[1]Faculty of Science, University of Kelaniya, Sri Lanka.
kaveefdo97@gmail.com*, sujeew@kln.ac.lk

In the twenty-first century, mathematical proficiency is crucial due to the widespread exchange of data and efficient communication across diverse fields. Data security employs encryption and various mathematical techniques to protect information systems. It safeguards against unwanted access, use, and damage. Graph theory is widely applied in the field of cryptography because a graph can be easily represented as a matrix on computers. The goal of this study is to make a novel connection between private key cryptography and graph theory principles that will safeguard data from unauthorized parties. In the encryption process, the original texts are converted into ciphertext by representing a splitting graph and using a minimum spanning tree, then computed into an adjacency matrix of ciphertext and partitioned it into a block matrix. Finally, obtained the resultant ciphertext using the receiver's private key. The decryption process follows a similar stage in reverse order. This suggested encryption algorithm demonstrates a new scheme for more complexity and security. The resulting ciphertext size is larger than the plaintext size and checked its validity.

Keywords: Cryptography, Decryption, Encryption, Graph Theory, Symmetric key Cryptography.